University of
Southern
Queensland

DATA PRIVACY AND SYSTEM SECURITY ON CLOUD COMPUTING ARCHITECHTURE FOR BANKING AND FINANCIAL SERVICES INDUSTRY

A Thesis submitted by

Abhishek Mahalle
(B.Tech., M.M.S.)

For the award of

Doctor of Philosophy

2023

ABSTRACT

To operate in cloud computing environment, organizations need to adhere to policies, procedures, and controls to deliver technology services to business system users. Despite following globally known frameworks and ISO standards, cloud computing architecture and cloud computing infrastructure remains to be under constant monitoring and assessment. Cloud computing infrastructure provides access to data and applications from any location, and this has made organizations (specifically Banking and Financial Services Corporations) to keep evaluating privacy and security frameworks. Banking and Financial Services Corporations have data and applications which are internally developed to remain ahead of competition. These data and applications become the Intellectual Property (IP) that serves specific business processes and goals. When these data and applications can be accessed from remote locations, there are a potential risks of data leakages and erosion of IP over a period. Data privacy and security of cloud architecture infrastructure continues to be the challenge across the globe and for Banking and Financial Services Corporations, where customer financial details are stored over system, the area continues to be of further importance. Considering these problems associated with cloud computing, this research develops a research question about risk added by cloud computing to data privacy and system security for Banking and Financial Services Corporations. This research includes survey in the areas of importance for cloud users while using cloud infrastructure for Banking and Financial Services Corporations. This thesis collects feedback from identified sample size of academicians and professionals from information, communication, and technology (ICT) background, for areas of cloud governance, cloud security and perception towards cloud computing for Banking and Financial Services Corporations. In this thesis, I have identified various issues and challenges faced by Banking and Financial Services Corporations and discussed the importance of governance & security required for these organizations. Upon reflection this research provides areas of constant monitoring, assessment and upgrades required for data privacy and security on cloud computing infrastructure. This research examines the current cloud architecture and infrastructure management and governance practices in Banking and Financial Services Corporations and concludes by providing detailed achievement of the thesis. This research concludes that managing data categories and application types is complex over cloud architecture. To manage this complexity, cloud architecture and infrastructure will continue to demand financial investment. This research further answers the research question that to enforce data privacy and system security, dedicated incident and problem management team, legal expertise to form cloud management contracts, dedicated team for managing cloud security penetration testing teams, dedicated human resources with relevant work experience, IT Risk management framework and alert & monitoring for ongoing use of cloud infrastructure will be required to measure and control cloud computing architecture and infrastructure. This research concludes to confirm quarterly review of roles and responsibility of cyber security executives along with security framework and governance structure. This research confirms need of dedicated budget, business continuity plans, ethical controls within cyber security teams and job rotation within cyber security executives. Cyber security executives must be continuously educated about recent cyber-attacks and potential losses incurred by other organizations. This research concludes that Digital transformation demand investment into new cloud infrastructure to prevent data leakages risk to customer data. Third Party cloud service providers plays key role in managing cloud security. Risk event and risk mitigation plans are mandatory for digital transformation. This concludes that there is need of specific technological tools and human skills to manage specific forensic investigations. This research also suggest that IT Security contract needs special handling in special investigation scenarios. This research also provides perception of the survey participants towards ease of cloud computing. The focus of this research is on practical utility providing researchers with results that are more readily endorsed, thus maximising the impact of the research findings in practice.

CERTIFICATION OF THESIS

I Abhishek Mahalle declare that the Thesis title *Data Privacy and System Security on Cloud Computing Architecture for Banking and Financial Services Industry* presented for examination is not more than 100,000 words in length including quotes and exclusive of tables, figures, bibliography, references, and footnotes. The thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work.

Date: 29 June 2023

Endorsed by:

Professor Jianming Yong
Principal Supervisor

Professor Xiaohui Tao
Associate Supervisor

Student and supervisor's signature of endorsement are held at the University.

ACKNOWLEDGEMENTS

There are number of people without whom this thesis might have not been completed. Firstly, I would like to thank USQ graduate research office for supporting this research. I would like to provide my deepest appreciation to Prof. Jianming Yong and Prof. Xiaohui Tao for providing all necessary support and guidance to complete this thesis. Without their supervision and expert guidance this thesis would not have been possible. I would also like to thank non-teaching staff of USQ who extended all possible help to complete this thesis.

This research has been supported by the Australian Government Research Training Program Scholarship.

CANDIDATE’S PUBLICATION LIST

During this research, several research papers were published. The publication list follows next.

CONFERENCE PROCEEDINGS

2018 22nd IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2018)	**Mahalle A**., Yong J., Tao X., “Data privacy and system security for Banking and Financial Services Industry based on Cloud Computing Infrastructure”, Proceedings of IEEE CSCWD 2018, Nanjing, China
BESC 2018, The 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing	**Mahalle A**., Yong J., Tao X., “ITIL Processes to mitigate Operations Risk in Cloud Architecture Infrastructure for Banking and Financial Services Industry”, Proceedings of the 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing, National University of Kaohsiung, Taiwan
2019, 23rd IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2019)	**Mahalle A**., Yong J., Tao X., “Insider Threat and Mitigation for Cloud Architecture Infrastructure in Banking and Financial Services Industry”, Proceedings of 23rd IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2019), Porto, Portugal
2019, 23rd IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2019)	**Mahalle A**., Yong J., Tao X., “Ethics of IT Security Team for Cloud Architecture Infrastructure in Banking and Financial Services Industry”, Proceedings of 23rd IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2019), Porto, Portugal
BESC 2019, The 6th International Conference on Behavioral, Economic, and Socio-Cultural Computing	**Mahalle A**., Yong J., Tao X., “Protecting Privacy in Digital Era in Banking and Financial Services Industry”, Proceedings of BESC 2019, The 6th International Conference on Behavioral, Economic, and Socio-Cultural Computing, Beijing, China

2020 24th IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2020)	**Mahalle A**., Yong J., Tao X., “Challenges and Mitigation for application deployment over SaaS platform on Cloud Architecture Infrastructure in Banking and Financial Services Industry”, Proceedings of 2020 24th IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2020), Dalian, China
2020 24th IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2020)	**Mahalle A**., Yong J., Tao X., “Regulatory Challenges and Mitigation for FinTech”, Proceedings of 2020 24th IEEE International Conference on Computer Supported Cooperative Work in Design (IEEE CSCWD 2020), Dalian, China
BESC 2020 The 7th International Conference on Behavioral and Social Computing, Bournemouth University (Virtual Conference)	**Mahalle A**., Yong J., Tao X.,”IT Investment Governance and Corporate Governance-Perspective and Approach”, Proceedings of BESC 2020 The 7th International Conference on Behavioral and Social Computing, Bournemouth University (Virtual Conference), Bournemouth UK,

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	**Full Form**
AISeL	Association for Information Systems Electronic Library
BESC	Behavioral, Economic, and Socio-Cultural Computing
B2B	Business-to-Business
CCM	Cloud Control Matrix
CMM	Capability Maturity Model
CMMI-SVC	Capability Maturity Model for Services
CMMI	Capability Maturity Model Integration
CC	Cloud Computing
CG	Cloud Governance
CSCWD	Computer Supported Cooperative Work in Design
CS	Cloud Security
CoM	Configuration Management
CobiT	Control Objectives for Information and Related Technology
DSS	Data Security Standards
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNS	Domain Name Server
ICT	Information and Communication Technology
IS	Information Systems
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organisation of Standardisation
KPI	Key Performance Indicator
MIS	Management Information Systems
NA	Not Applicable
NIST	National Institute of Standard and Technology
PDF	Portable Document Format
PM	Problem Management
RQ	Research Questions
SERVQUAL	SERVQUAL Service Quality
SLM	SLM Service Level Management
SM	Supplier Management
USQ	University of Southern Queensland

CHAPTER 1: INTRODUCTION

1.1 Chapter introduction

The research developed a survey to identify key requisites for cloud computing infrastructure to operate for Banking and Financial Services Corporations. This research highlights risks added to data privacy and system security. This research proposes the need of additional infrastructure and more efficient way to manage cloud computing architecture and cloud computing infrastructure. This research was conducted at University of Southern Queensland (USQ). A Case of Bank, its critical cloud infrastructure was considered for evaluation of the research artefact. This section introduces the research. Background information and the motivation behind the development and proposal for more efficient way to manage data privacy and system security for cloud computing architecture and cloud computing infrastructure in *section 1.2*. Next, *sections 1.3 to 1.8 provide* supporting details for data privacy and system security. Next the research problem and associated research questions are stated in *section 1.9*, followed by the justification of this research in *section 1.10*. The research methodology is then outlined in *section 1.11*. Finally, the scope delimitations and key assumptions are stated in *section 1.12* and the format of this thesis is outlined in *section 1.13*. *Section 1.14* provides the chapter summary as the conclusion to this chapter.

1.2 Background and motivation

This section sets the scene for critical understanding of the research context. For cloud architecture and cloud infrastructure to provide desired services to business system users (employees, customers, 3rd party technology service providers) the specific frameworks to govern cloud (example COBIT, ISACA, ITIL) and cloud security reference architecture (example NIST, CCM) are followed by corporations across globe. Following these frameworks have become crucial to deliver business value of IT. As IT is deeply intertwined in business processes, both business process and IT follow these frameworks meticulously. These frameworks are aligned with business operations and IT by identifying and making appropriate improvements. However, despite following these frameworks, there are still complexities involved in managing cloud computing resources (cloud architecture and cloud infrastructure). From review literature, very little has been proposed on how each organization uniquely aligns these frameworks for IT value delivery. Each organization performs self-assessment of the IT services delivery through IT Audit services. This self-assessment (IT Audit) includes data privacy and system security related aspects. This is where this research helps to provide data privacy and system security teams about risk associated with cloud computing resources (cloud architecture and cloud infrastructure). This research includes feedback from academicians and professionals with knowledge of cloud computing and background of ICT.

1.3 Data privacy and system security for banking and financial services industry

Cloud computing has deployment models defined based on type of availability of cloud computing resources and accessibility. Main deployment models for Cloud computing are private, public, hybrid, community, inter-cloud and multi cloud. Banking and financial services industry directly works for economy and so remains matter of national importance and for livelihood of people. As a part of security implementation in bank's technical infrastructure various security checks in the form of digital certificates for devices, one time password token, browser protection policies, transaction monitoring, anti-money laundering and fraud detecting systems are in place. These devices and systems give robust security measures for the banks at the same time they meet the regulatory requirements to protect data of the customers. With evolution of internet, corporation operating in Banking and financial services started offering their products and services via internet-based platform and machines (ATMs) located in remote locations without making customers to visit its branches. These online banking services offers flexibility and convenience in access to banking services. Banks and financial services offer variety of financial products and services to its retail & corporate customers that include internet banking services, mobile banking facility, ATM withdrawals & deposits, Credit card facilities, Debit card facilities, EFTPOS terminals, account maintenance services, stock market and treasury products and forex service. These services can be availed without visiting the actual branch of the bank. These products can be accessed via internet. This helps bank to achieve operational efficiency through faster delivery of services, reduce cost of operation of branch, work with lesser staff, provide competitive services, make faster decision in real time for customers and focus on customer needs to offer personalised services (Mahalle et. al., 2018). Through cloud infrastructure banking and financial services also meet regulatory & compliance of central bank. When the technology infrastructure offering these services is located at secured site and both staff & customers accessing it from various remote locations – data privacy and systems security continues to be the top priority with zero tolerance for risk.

1.4 Protecting privacy in digital era

With a 3rd wave of digital transformation after industrial revolution and wide spread of internet across globe, we have mass adoption of product and services available over connected and well networked digital devices. Never in history had so many people connected and available, at the same time communicating and responding to digital content.In this consistently emerging world where digital devices equipped with sensors have become medium to collect information, both consumer and producer want to take advantage of available information and use it for profit (monetary or otherwise). Through digital transformation, corporations want to make use of consumer available over internet, route the internet traffic towards their product & services and drive sales. The digital transformation came out to be primarily sales strategy and then consumer convenience.

For Banking and Financial Services, application on digital devices provide several services that include convenience for payment, able to check account balances in real time, locating ATM without using map, locating nearest branch to report issue with accounts (and cards), generating online statement and ordering legal documents & card. This improves perceived usefulness and perceived "Ease of use" of banking services over digital devices (Mahalle et. al., 2019). The data generated by bank’s customer is mostly financial in nature and is collected through “consent form” signed / accepted by customer. When this financial data is related with data generated over other digital platforms, it provides key insights about the customer’s behaviour, which can be used to create customer specific product and price it to sell. At this point, customer may treat this as “emotional manipulation” and may not want to receive suggestion about new product and services and may not want Bank to use information from other digital platforms. This is where Banking and Financial Services Corporations need to be careful in providing suggestions over digital devices through their applications.

1.4.1 Impact of privacy breach

The use of knowledge generated by consumers is impacting general lives of individuals / consumers. The impact is in the form of material and immaterial loss. Material loss of personally identifiable information and immaterial loss through loss peace of mind and psychological discomfort. Below are the areas identified showing impact due to loss of privacy: (Mahalle et. al., 2019)

1. **Intermittent or regular annoyance while using digital devices and platforms (Psychological Discomfort)**: While browsing websites, the website show advertisements which relates to item purchased or services availed in recent past, location visited, stores visited and website searched for information. These advertisements are sometimes regular or intermittent which are not relevant to existing needs. The advertisers used old digital footprints to predict future needs and generate sale.
2. **Emotional manipulation**: Based on digital footprints advertisers select product or service which are similar and are closely related to most recent activity over digital platform. This removes the chance of consumers willing to browse more product & services and new products. Consumer treats this as an emotional manipulation.
3. **Selective participation over internet**: The constant use of digital footprints to predict and propose product and services leading to emotional manipulation forces consumer to hold from communicating views and thoughts over digital platform. The consumer loses freedom of expression considering use of information in future to make behaviour prediction.
4. **Loss of anonymity**: The digital footprints collected from various sources (Ecommerce website, social media platform, video streaming websites) and relating them to identify user (first name, last name, email address, employment details, postal address). When these details are used to target individual with an advertisement, the consumer feels ‘known” point of target. Consumer feels loss of personal information to unknown source and may become target in future again.
5. **Behaviour guidance / target for specific product or service**: The digital footprints are used to guide an individual’s behaviours and actions due to known

past and present circumstances. This makes an individual feel loss of privacy, being watched constantly, correction in actions when not even asked, receiving unasked for advice and loss of sense of self. It makes an individual lose peace of mind and freedom to think.

6. **Stolen private information**: The digital footprints can be collected from various sources and combined to known complete details of an individual. Information available on digital platforms like photo, birth date, email address, employer, photos of gifts items have name written on it is available online, home address, affiliated groups (social, political, educational, charitable), social security number, credit card number and organizations (corporation offering employment and related services), mobile phone number, video and home phone number, can be used for identity theft, create bank savings and loan accounts and used to apply for credit card. This may cause huge financial loss to the individual.

7. **Email account hijacking**: Various online ecommerce platforms ask to provide email to avail services. For example, the food ordering digital platform ask to provide email address to avail discounts and coupons. The discount confirmation and digital coupons are mailed to customer. Once the discount or coupon is used, it provides additional information about an individual and helps verifying the email address. If this email addresses are used for unauthorised login and hijacked, they will cause tremendous loss of information of an individual.

8. **Social media account hijacking**: Social media platform use email address or phone number to login. The digital footprints collected from various sources can be used hijack social media account and use to post derogatory comments, to spread fake news, to provide false information, to create confusion to related members over social platform and mislead them, to know confidential information which an account owner can reveal only to concerned people or groups and to know where about of the people which are friends, family or world colleagues. The account can be hijacked to know bank and other financial details.

9. **Price manipulation and lowered competition**: There is process being followed to use digital data which involves collecting information from various digital platforms, analysing information to understand consumer behaviour, taste and preferences, creating personalised product, digital content and advertisement,

pricing product as per spending habits, and generating sales for company. The process involves knowing buyer, colluding to create product & price and creating most lucrative offer. If the data used to create this offer remains with only one type of product or service, they will keep other companies offering similar product and services and keep competition away. This not only leads to unfair competition in economy but also leads to steering preferences of customer. This process can be applied to any products of insurance companies or other companies in industry.

10. **Segmentation and advertising**: The various digital footprints collected help to divide consumer based on several basis like gender, education level, income level, employment industry and marital status. This division help to target consumer based on trend in economy and individual taste & preferences.

11. **Loss of trust and civil liberty**: The use of digital footprints to constantly analyse, make predictions on future actions and guide an individual's thought makes him / her be under control of unknown source over digital platforms. The basic right to live with liberty, at peace with thought & actions (real or virtual world) and freedom of expression is diminishing.

12. **Constantly under supervision (or digital surveillance) and security issues**: The digital footprints generated and left-over digital data storage devices in the form of location data through use of maps and itinerary planning application, provide enough information about place of physical presence. This location data when used to combine with surveillance camera, can acts evidence about an individual's location at specific moment of time. When this data is misused, it will lead to invasion of privacy. This will produce a reaction and new behaviours which are expressed by individual's exposing digital platforms to surveillance using digital technology.

13. **Reverse engineering on personal details through digital footprints under the cover of personalised experience**: Apart from digital footprints being used to provide suggestion and better buying decisions, the analysis is investigating personal information and behavioural traits. Through data analytic tools, every transaction (monetary or otherwise) is read and analysed to arrive a logical

conclusion and action plan; this is constantly engineering to manipulate an individual’s thought and actions.

14. **Insensitivity about customer and their data**: After the digital footprints of all forms are collected, the data analytics and digital advertising firms have very little or no concern for data and its usage. The data is used for all possible purposes and to the maximum extent until new data (suggesting new behavioural patterns) about an individual to generate sales. It is only the perceived threat of loss of data and identity is which concerns to an individual. The data may be simple information for data analytics companies and advertisers; however, same information may be critical to an individual.

15. **Victim of online scam / lost money**: The spammers, online advertisers and fraud lottery companies collect user data under legitimate entities or through legitimate entities and use it to target masses to make money. An individual having no role in providing information directly to any of the companies becomes victim of fraud and losses money, reputation, time and critical information that can be used again if not completely removed from servers.

16. **Online data and location details that create danger and risk to life (Digital trail-monitoring to analyse and interpret individual’s private association and relationships with various people and / or places)**: The digital footprints collected by people from past life, former romantic partners and divorced or separated couples under court case, can be used to locate and pose threat to an individual. This may lead to risk and danger to one’s life. The digital footprints when misused may pose threat to physical security of an individual.

17. **Driving ecosystem for an individual through digital data**: The digital footprints collected from several sources are used to make prediction about future needs and propose product & services, use location data to gauge travel patterns, locations of interest, relate to available products (brands), use social media comments, likes, dislikes, content shared and content hide or reported to provide selected advertisements. The over financial, social and economic life cycle around an individual is driven through news feed, tips and suggestions. Both mental and physical space is controlled which makes an individual have lesser or

no control over their life. This is pushing an individual to surrender to their digital world to live in a material world.

18. **Distribution of information**: The digital footprints are collected, stored, cleaned and are “traded” through various companies having vested interested in data. The interest on these entities can be sell data to product companies to political group to gauge demographic details. The data generation can be at one geographical location and distribution at other geographical location, this makes data may be secure at one place with no guarantee being secure at other location. The digital data being easy to copy and distribute, the control over data from individual is lower and negligible.

1.4.2 Protection of privacy

Having understood the importance of data privacy and implication of its loss, it becomes imperative for Banking and Financial Services Corporation to collect data of its customer responsibly from own information systems and 3rd party data analytic companies. Banking and Financial Corporation are imposed huge financial penalties and face cases with Banking Ombudsman for not complying with data privacy regulations. To enforce new controls, Banking and Financial Corporation, below proposed steps: (Mahalle et. al., 2019)

a. **New consent form for data collection and application usage policy (notice)**: The new consent form needs to be designed which will show additional “paragraph” about external sources that may be used to collect customer data, need to collect, store, analyse this data. Banking and Financial Services Corporations need to re-design digital platform / application to provide additional functionality to notify user when data is collected, source of data and its intended use. This will bring transparency and objectivity in application usage and data collected. This will keep customers informed about advertisements over digital platforms and will improve Sales & Marketing strategy.

b. **Selective data sharing by customer (choice)**: Banking and Financial Services Corporations proactively have to inform customer over application for “not using” the customer data, requests customers to provide information about financial needs, develop and inform customer about additional page for data collection and data collection set up, propose to use data based on customer request through digital platforms, inform customer about data type (social, ecommerce, location) collected from platforms and if it is required, should request customer to select duration for which data can be collected and used (including historical information – if available), frequency of data collection and analysis, and informing customer about data source (internal or external). These steps will put customer in complete control of data, even if it is outside the information system of Bank. This will develop trust and better image of Banking and Financial Services Corporations. These measures will also help to support and develop personalised experience over digital platforms. Though this step will give minimal visibility about customer insights, however, will safeguard customer interest.

c. **Degree to which private information used**: Once the bank's customer confirms need and allows to use private information collected from various resources, it is clear to both Banks and customer for intended use and duration of its use. The suggestion offered to customer will clarify degree to which private information was collected and used. This brings transparency in use of private information. This will help mitigate risk of prolonged use and ongoing access to digital footprints of customer.

d. **Do-Not-Call-Registry to Do-Not-Track-Policy**: With the popularity and growth of mobile phone connections, the telemarketing advertisement became very common which annoyed several people across the globe; to relive the stress, governments forced a rule for telecom operators to introduce "Do Not Call Registry" portal which listed mobile phone numbers. Once the phone is registered, it cannot be contacted for telemarketing purposes. In digital era, we need "Do Not Track Policy" rule to prevent collection of digital footprints. An online portal which will act as first check if the mobile phone (or any other handheld device that can be used to connect on digital platforms) can be used without owner's permission to collect digital footprints. Also, Banking and Financial Services Corporations can be proactive to introduce this policy and inform customer over customer platform through consent form.

e. **Business customer and technology relationship**: An individual's use of mobile devices over digital platform for personal purposes and same individual being the consumer for various product services are two different domains. These domains are separated by an individual’s choice and an individual can decide to let 3rd party data collector migrate “to and fro” between these domains. Banking and Financial Services Corporations (along with others) have to let their employee and data analytics services provider know this truth very clearly by constantly educating about customer privacy, new methods to breach the privacy and implication to company and customers.

f. **Need of cloud platform adaptable to new technologies**: The constant evolution of economy and alignment to digital transformation under the supervision of regulatory environment requires adopting to changes. These changes when requires technological adoption involves new encryption mechanism, updated firewall rules, deploying security features to know new threats and vulnerabilities, prevention of data transfer across globe by eliminating file transfer protocols and developing datacentres to retain data within the geographical boundaries of customer. To meet these requirements that deal directly or indirectly to protect privacy of customer, cloud platforms should be ready to deploy, maintain and support new technologies. At the same time, a regular monitoring and alert mechanism will be required to plan and implement if new technologies emerge.

g. **Agile environment and cultural transformation**: The digital era has brought below key changes for Banking and Financial Services Corporations:

   i. Enabling Digital platform to change channels of interaction between bank and customers – voice enabled GUI.

   ii. Change in work (everyday task) due to change in work and task coming through digital platforms.

   iii. Digital platform offering key front end / customer facing services and operation back end (office procedures) is handled by different teams in Banks.

   iv. Effectively using digital channels by Bank to deliver customer needs – division between traditional email, phone call, PDF documentation and self-serving menu items in digital applications

v. Focus on specific areas of innovation to offer product and services.

vi. Proactively embrace regulation to safeguard bank and customer.

vii. Optimise the digital footprint throughout the customer journey over digital platforms.

Above changes need educating internal staff and 3rd party vendors about Privacy, Societal and Ethical Issues of digitization that impact customer. Re-design of business model, reconceptualization of business activity, tasks for digitally enabled customer will also bring awareness in customer about steps taken to enforce privacy protection and data security.

The collection, storage, cleaning, merging, analysis and use of digital footprints of customer for providing suggestions to drive sales of business are not 100% correct way of providing convenient digital platform. The use of digital footprints on "customer's need" basis and upon permission from customer is where Banking and Financial Services Corporations can bring greater transparency, protecting privacy and win trust of customer. The knowledge generated by customer over digital platform continues to be proprietary information of the customer and customer have complete rights to its retention and disclosure. Considering this, control measures to collect, store, analyse and use digital footprints of customer must be incorporated by Banking and Financial Services Corporations. Banking and Financial Corporations needs to carefully assess the digital strategy if it will generate economic activity and generate sales.

1.5 Operational risk management and ITIL method to prevent breach of privacy and loss of private data in cloud architecture infrastructure.

With global adoption of private cloud architecture infrastructure model by Banking and Financial Services Corporations, control over changes to its hardware, software, applications, databases, telephony, network, and security layers are part of everyday IT operations management. As a part of IT Operations processes, various issues reported by cloud users are investigated and fixed to maintain the information system's integrity and accuracy. IT Operations follows the global terminologies and procedures as defined in information technology infrastructure library (ITIL). The ITIL briefly explains and guides main tasks of IT Operations. The primary tasks of IT Operations include incident management, problem management, risk management, financial management, capacity management, release management, configuration management, service level management, IT service continuity management, availability management and change management processes with key stakeholders. These processes together help to operate, maintain, and monitor cloud architecture infrastructure. (Mahalle et. al., 2018)

ITIL processes helps to reduce cost and better management of IT operations service delivery. ITIL processes help to prepare response for various issues reported by cloud users, categorise & prioritize issue based on risk and impact, develop solution, implement solution, mitigate any risk arising due to failures and restore services for business service continuity.

IT Operations in Banking and Financial Services Corporations operate within the governance framework defined by ITIL (Mahalle et. al., 2018). ITIL provides the process map for everyday operations to ensure processing enabled over technology meets its desired result. The resolution implemented through ITIL framework through technology also help govern the future behaviours and adjustment required in technology when there is need of meet objectives of business activity.

1.6 Insider threat and mitigation for loss of private data

Insider in an organization is referred as the trusted employee or third-party contractor who has legitimate access to cloud infrastructure. These insiders when exploits the cloud vulnerabilities with an intent of making financial gain or causing reputational damage to organization or disrupting the business; it impacts both business and culture of the corporations. Considering sensitivity of the incident related to loss of private data of organization and is customers, most of the cases are isolated from the employees and are not made public. However, based on nature of system exploitation of system and vulnerabilities, additional security controls, organization policies and employee education programs are developed. Banking and Financial Services Corporation constantly strive to take a holistic approach to deal with people and situation. Considering the nature of work and need to deal with confidential customer and financial data, trust level is established with employees and third-party contractors by the organization. With *insider* as an employee, organization policies are used as control methods; for Third party contractors' contractual agreements and monetary penalties are enforced as control methods. (Mahalle et. al., 2019)

Considering the importance of *insider* and their roles and responsibility for business operations though information systems, it is important to define *insider* types and associated risk (possible chances of fraud or exploitation) with information systems, this help in developing counter measures as risk mitigation approach. Counter measures can be preventive, deterrent, detection, and recovery.

Types of insiders in Banking and Financial Corporations based on cloud users (Mahalle et. al., 2019):

a. An insider can be an employee operating from Bank’s branch or head office and an intern (part time / full time) with legitimate access.

b. An insider can be third party cloud service provider with Admin access to computing devices.

c. An Insider can be third party auditor.

d. An Insider can be a business partner for short term services like legal consultants, business consultant, property developer and supplier, sales agent / broker / dealer with a formal relationship with Bank.

e. An Insider can be Bank’s customer who can access Bank’s specific applications through legitimate access.

f. Anyone who acts on behalf of employee, whom insider has given credentials (user id and password)

g. Anyone who is forced to perform actions on behalf of insider.

h. A former insider who no longer work for Bank, but access was not removed during employee separation or insider who creates another access while working for bank and then leaves the Bank.

Each of the above insiders can harm the data and information systems through misuse of access and bypassing the defence mechanism. Considering the insider has already gained access, it’s the misuse of the system that leads to data leakages and information loss. The level of access determines the extent to which data and information systems are damaged.

The known path to the access information & computing devices and methods to exploit the vulnerabilities in short period of time is what adds risk because of insider. This is also called skill level of the insider.

1.7 Ethics of IT security team to protect privacy

Ethics refers to the moral standards that help guide actions, choices, and behaviour on individual or group. Ethical choices, decisions and behaviours play crucial role in the situation which involve element of risk, need of truthfulness, honesty, and reflection of one's character. In Banking and Financial Services Corporation, *ethical* standards play an important role in building a brand value and lasting reputation in industry supporting to prevent privacy of customers and loss of data. In Banking and Financial Services Industry, "Code of Practice" defines the standards of offering services and method of operations, however, it's the ethical standards of CEO, board of directors and employees that reflects the extent to which "Code of Practice" is adhered to in everyday life. (Mahalle et. al., 2019)

In Banking and Financial Services Corporations, Operating on Cloud architecture and role-based access control methods, where data and applications are available, based on level of access and criticality (and confidentiality) of information, ethical standards are required from all the employees to ensure information systems' confidentiality, integrity, and availability. (Mahalle et. al., 2019)

Ethics for employees of organization are guided by moral principles / commandments. Below are moral commandments for information security:

1. One shall not use a computer to harm other people.
2. One shall not interfere with other people's computer work.
3. One shall not snoop around in other people's computer files.
4. One shall not use a computer to steal.
5. One shall not use a computer to bear false witness.
6. One shall not copy or use proprietary software for which you have not paid.
7. One shall not use other people's computer resources without authorization or proper compensation.
8. One shall not appropriate other people's intellectual output
9. One shall think about the social consequences of the program you are writing or the system you are designing.

10. One shall always use a computer in ways that ensure consideration and respect for your fellow humans.

Above principles guide the actions, behaviour, and decision of employees throughout the organization to promote ethical use of information systems and access level. However, it’s the *ethical dilemma* to make correct decision in the event of having revealed private / confidential / secret information of an individual and / or of an organization is what confuses employees and tests their ethical standards.

Ethics based on context and case can be categorised on following types:

1. Descriptive Ethics: It is the factual study of the ethical standards or principles of a group or tradition.
2. Normative ethics: It is the development of theories that systematically denominate right and wrong actions.
3. Applied Ethics: It is the use of above theories to form judgments regarding practical cases.
4. Meta-Ethics: It is careful analysis of the meaning and justification of ethical claims.

In Banking and Financial Services Corporation, having established the ethical framework, it is the field of “applied ethics and Meta-Ethics” that is useful to deal with everyday situations.

Table 1: Ethical principles and ethics of IT security team (Mahalle et. al., 2019)

Ethical Principles	Ethics for IT Security Team
One shall not use a computer to harm other people	IT Security Team despite having access to block access of Cloud User and send mail from Security Mailbox; should not do it unless requested by HR or Disciplinary Action Team
One shall not interfere with other people's computer work	IT Security Team despite having access to check details of files, folders, emails and messenger logs, should not see work on another employee's computer
One shall not snoop around in other people's computer files	IT security Team should not copy, modify, or delete files from other employee's computers

Ethical Principles	Ethics for IT Security Team
One shall not use a computer to steal	IT Security Team should not use access to copy private or confidential information of an employee without requesting to an employee or unless requested by HR. IT Security team should not use access to copy information that would have been unauthorised for in normal circumstances.
One shall not use a computer to bear false witness	IT Security Team should limit their role in investigation to providing information and logs; IT security should not make decisions for case.
One shall not copy or use proprietary software for which you have not paid	IT Security Team should use and allow users of cloud to use only Paid software applications.
One shall not use other people's computer resources without authorization or proper compensation	IT Security team should not use other employee's network storage and hardware components without informing and making appropriate payments.
One shall not appropriate other people's intellectual output	IT Security Team should not use other employees' intellectual property or copyrighted materials for self-gain
One shall think about the social consequences of the program you are writing or the system you are designing	IT Security Team should perform the risk assessment of security policies implemented and their impact on employees & organization culture
One shall always use a computer in ways that ensure consideration and respect for your fellow humans	IT Security Team should not misuse their access to gain access to private information of other employees and use it to cause disrespect.

1.8 Regulatory challenges and mitigation for privacy issue in new digital platforms offered by banks

With rapid development in network connectivity, use of mobile phones for surfing internet and the use of mobile phones to access bank services has evolved from mere providing payment services to more sophisticated data driven business models. By analysing the large amount of historical data available from banking services systems availed over mobile phones and combining it with similar amount of data available from other internet platforms by customer provides key insight about customer's private information; this includes personally identifiable information, customer demographic details, customer taste & preferences, demand and consumption of goods & services, travel habits & frequent travel destinations, inclination towards various causes like environment, communities, politics and participation in events. All this information about an individual can be used to provide products and services of bank, to improve financial activity for customer or group of customers, to develop product and services only for identified set of customers, to offer more sophisticated products (SME Payment services, Payment channel for wealth management, peer to peer lending, forex remittances and crowd funding platforms), to improve customer experience at the same time generate profit for Banking & Financial Services Corporations. However, considering the demand from regulators and consumer protection laws to provide "Substantive Fairness" while offering product and services, it becomes mandatory for Banking and Financial Services Corporation to remain within boundaries of Acts and Laws (Mahalle et. al., 2021). The innovation in business model and financial product & services requires alternative approach to regulatory boundaries. Innovation in financial services further requires meeting regulations specific to country. The engineering in financial products and developing product offerings serviceable over mobile devices may lead to fast adoption and rapid growth in financial markets, which also paves way for systemic risk due to misconduct in lending practices. Considering all these aspects, developing technology platform that meets all the "minimum regulatory requirements", yet, modifiable to support additional requirements due to "innovative" nature of business model becomes a better approach for "Digital Platform" to serve in marketplace. The "incremental regulatory framework, for iterative business model" in financial services industry sets the theme for growth, scalability, and sustainability of digital business model. However, financial institution holding authorised deposit taking institutions (ADIs, Banks) licenses have market access (established trust with customers, insurance for deposits and customer base), while Bank's digital platforms have technology access (sophisticated data analytics tools, innovative business model, lower cost of operation, no need of acquire full bank services and thus save license fee). (Mahalle et. al., 2021)

1.8.1 Challenges for account related services provided by Bank's digital platforms and area of customer privacy exposure

The key challenges for Banks, is to design online platform and operate bank at the same time deliver product and services through platform over mobile devices.

Table 2: Challenges faced by banks. (Mahalle et. al., 2021)

Goals of Bank Product & Service Design	**Business Model and Regulatory Design Challenges**	**Bank's Operating Challenges**
Low Margin	Volatile	Cost
Asset Light	Uncertain	Service Channel
Scalable	Complex	Quality and Efficiency
Innovative	Ambiguous	Privacy, Security and Risk
Compliance light		Service Model

The elements mentioned in above table, their permutation, and combinations from design phase to operating phase during life cycle of financial product & services are considered before it is made available to customers (Mahalle et. al., 2021). These elements need to be considered for below critical life cycle of product & services:

1. Diligence in customer identification and rational behind customer identification
2. Disclosures about product & services, Terms & conditions, applicable fee, interest rates, duration of contract and associated risk with funds to customer - From marketing (quote assistance) To after sales service (credit assistance)
3. Document submission and document generation

4. Contract acceptance and digital signatures
5. Payment Gateway availability for fund transfer and receipts
6. Account Operation Services provided during “life of a contract”.
7. Communication channel between customer and financial services providing entity for timely redressal of complaints.
8. After sales Risk Management Framework for Interest rate risk and non-interest rate risk
9. Report generation and reporting framework as per product for customer & Banks
10. Insurance Facility available for product and services
11. Terms & Conditions as per Business Model including applicable service fee, amount calculation methods / formulae, net interest rate applicable.
12. Additional Account Services available related to existing products (Cross sales mechanism)
13. Account closure and contract termination details
14. Providing Hardship Notice to customer and working for credit products
15. Data storage and retrieval within Bank’s digital platforms form and from outside sources (including for Key Fact Sheet)

The above discussed elements of design and life cycle of product & services need to meet legal framework that covers Corporations Act, Consumer Protection Law, Criminal Law / Crimes Act, Electronic Transaction Act, Trade Practices Act, Privacy Act / Financial Sector (Collection of Data) Act, Competition and Consumer Act, Consumer Credit Protection Act, Responsible Lending Guidelines and Securities & Investment commission Act, Anti-Money Laundering and Counter Terrorism Financing (AML-CTF Act) and Financial Crimes Investigation Reporting, Interest Rate and Non-Interest Rate Risk.

1.9 Research problem and research questions

After an introduction of the research context and an understanding of the motivation behind this research, the objective of the research is:

To identify if cloud computing will continue to bring risk to data privacy and system security for cloud architecture and cloud infrastructure of banking and financial services corporations.

Based on the objective, the research problem can be formulated as below:

There is a risk associated with data privacy and system security on cloud computing architecture of banking and financial services corporations.

To address this research problem, an understanding of the challenges of the existing cloud architecture and cloud infrastructure is required. This leads to the overarching research question for this research:

What are the factors that add and mitigate risk to cloud architecture and cloud infrastructure of banking and financial services corporations.

The overarching research question is broken into five specific research questions (RQ1 to RQ5) for granularity and clarity:

In the context of the research the first research question seeks to identify impact to data categories and applications over cloud computing architecture:

RQ1: What will be the impact to the various data categories and application types used by banking and financial services corporations due to cloud architecture and how it will impact the business and customers?

The second research question seek to identify measures and controls required to protect cloud architecture:

RQ2: What type of measures and controls will be required for cloud computing architecture for banking and financial services corporations to enforce data privacy and system security?

Following second research question, the third question identifies the role of executives involved in providing secure cloud architecture:

RQ3: What will be the role of cyber security executives, security framework and governance structure to improve cloud security of banking and financial services corporations?

The fourth question considers view of digitization adopted by economies and seeks to identify risk to data:

RQ4: What will be risks to customer data due to digital transformation in banking and financial services industry?

The fifth question seeks to answer capability of cloud computing architecture to serve to specific needs of department in Banks:

RQ5: How will cloud architecture support need of specific departments from bank for forensic investigation purposes of banking and financial services corporations?

Outcome of these research questions is largely dependent on the activities defined in methodology. A detailed account of the evaluation and research methodology is presented in chapter 3 and 4.

1.10 Justification for the research

Moving from the explicit understanding of the research questions in the previous section, this section justifies the need for the research and provides an overview of expected contributions to research and practice. Research on cloud computing architecture in organizations has a predominant focus on strategic issues such as business-IT alignment and key performance indicators and associated risk. data privacy and system security on the other hand, focuses on delivery and Improvement that sits at the operational management level. Even though the data privacy and system security concept has been recognised to have important strategic implications, it has received limited academic interest regardless of growing industry adoption. A review of recent data privacy and system security research literature provides a research agenda to focus on new data privacy and system security model implementations and demonstrates a lack of theoretically driven research. Consequently, there is a need for academic research on innovative data privacy and system security initiatives and their real-life implications. Academic research on data privacy, data security and cloud service quality has concentrated on conducting gap analysis between customer expectations and perceived service quality using a service quality instrument from the marketing discipline called SERVQUAL. One of the most prominent Information Systems (IS) journals, MIS Quarterly featured several articles discussing the application of SERVQUAL as an IT service quality measure. There is a lack of research on the intrinsic data privacy and system security attributes relating to the activities undertaken before or during cloud service delivery. In other words, there is a lack of research in data privacy, data security and risk measurement. Business users rely upon cloud services to accomplish their tasks. It therefore makes sense that examining how a user works, i.e., processes, is an important measure of cloud service quality from a business perspective. Internal business processes are presented as one of four strategic pillars for business performance management in the Balanced Scorecard (Kaplan & Norton 1992). However, limited process measurement initiatives for data privacy and system security are reported in the literature and most frameworks borrow concepts from the software engineering discipline. It can be concluded that academic research regarding a transparent method to measure data privacy and system security is scant. One of the methods to determine data privacy and system security is to determine process capability by checking compliance with a standard. No concrete solution is presented in the academic and/or practitioner community to address these shortcomings. Therefore, it is worthwhile to develop a transparent and efficient method to conduct data privacy and system security assessments. This research addresses the need for academic research that can also be applied to practice, thus providing a rigour-relevance balance to propose a transparent and efficient method in data privacy and system security assessments.

1.10.1 Expected contribution to the research

To operate in a highly competitive business environment, organizations require the support of continually improving services from their IT departments. Even though the primary objective of data privacy and system security is to support business operations, the value of data privacy and system security for a better business-IT alignment has been reinforced at a strategic level. ITIL and ISO/IEC 20000 adopt the process approach principle of quality management (ISO 2012) to manage activities as processes. It is important to understand the benefits of data privacy and system security parameters to an organization. However, process improvement initiatives are hindered by a lack of empirically validated yet actionable design theories for a transparent and efficient assessment of data privacy and system security. As reported earlier, the motivation for this research arose out of the dearth of academic research in cloud assessment. The process assessment standard is relatively new in the data privacy and system security. Therefore, the expected contribution of this research is to address the need for a more transparent Data privacy and system security method based on ISO/IEC 15504, thereby serving as an industry trial for the new standard assessment model.

1.10.2 Expected contribution to the practice

In reviewing available literature, it appears that there is a strong desire to continually improve data privacy and system security but the lack of a continuous assessment method, along with cost, time and resource constraints prohibits regular assessments. The key driver of this research is to propose a better measurement instrument that supersedes the existing approaches for data privacy and system security assessments. The expected contribution to practice is to address the challenges reported by IT practitioners regarding high costs and the lack of transparency of existing data privacy and system security assessment methods. Identifying the key risk areas added to data privacy and system security and their remediation will enable practitioners to conduct consistent and replicable data privacy and system security assessments at a minimal cost securing the cloud architecture and infrastructure. Ultimately the areas identified are expected to enable practitioners to focus on the new areas of improvement efforts required. Moreover, by proposing a fine grained and actionable data privacy and system security approach, this research is expected to demonstrate a research practice that incorporates readily validated research artefacts that can be easily corroborated by practitioners.

In summary, justification of this research is presented in terms of its relevance to respond to the current industry challenges and in terms of its rigour to contribute to the wider body of knowledge with an empirically validated method. The research is also expected to contribute to practice since practitioners can receive information intensive, unbiased, consistent, and timely guidance in determining new areas of improvement.

1.11 Methodology

This section provides a brief overview of the quantitative and qualitative research methodology chosen to address the research problem. Further details are provided in Chapter 3 Research Methodology. To address the research problem stated in *section 1.3*, it was decided that a new and fine-grained quantitative assessment method should be designed and evaluated. A quantitative method places emphasis on achieving clarity in the goals and underlying theoretical constructs of a risk areas and carefully evaluating how well the new risk areas are managed by organization. A qualitative method focuses on achieving perception towards cloud computing. This research demonstrates how quantitative and qualitative survey methods are most suited to identify existing challenges with data privacy and system security.

In summary, guiding principles of quantitative research and qualitative research are followed to conduct this research.

1.12 Scope delimitation and key assumptions

This section explicitly states the key assumptions undertaken and scope delimitations for this research. The research was limited in terms of geographic location, time and assessment models used. Due to the temporal constraints of the research study, only studies data privacy and system security and security related areas of risk. These two areas studied are most common areas for organization and differ for every organization keeping the major risk areas same. The risk areas studied provide the reasonable scope for this research. Including other areas will demand more time to develop and conduct surveys. However, the efforts will be less fruitful with repetitive work of following same methods.

1.13 Outline of the thesis

The thesis is structured based on the DSR publication schema proposed by Gregor and Hevner (2013) and has seven chapters.

Chapter 1 (this chapter) provides the background and motivation to undertake this research. Justification of the research, statement of research problem and research questions, overview of research methodology, key definitions and scope delimitations of the research are also provided.

Chapter 2 examines prior approaches in the research literature and practice for cloud data privacy, cloud security and governance models assessments and highlights the gaps in literature; a summary of current research is provided in order to identify research opportunities. Finally, a case is made to develop the research model to proceed with the research work.

Chapter 3 describes the quantitative and qualitative methodology used in this research. The research philosophy, research design and research methods are described in detail, along with ethical issues considered in this research.

Chapter 4 presents a discussion of the research findings for research questions RQ1 to RQ5. The chapter provides a critical examination of the research results with discussions based on the context of the research method and reviewed literature. **Chapter 5** summarises the findings of the research and how this research addressed the research problem. The contribution of research to the body of knowledge is discussed and implications of the research to theory and practice are presented. Then limitations of the research and directions for future research are presented.

1.14 Chapter summary

This chapter laid the foundations for the thesis. The research background and motivation were presented for an overall understanding of the research context. Then the research problem and research questions were identified. Justification of the research and the research methodology was then briefly introduced. Key definitions and scope delimitations were provided before an outline of the thesis chapters. Upon this groundwork, the thesis can proceed with a detailed description of the research.

CHAPTER 2: LITERATURE REVIEW

2.1 Chapter introduction

Chapter 1 introduces the research problem: there are new risk introduced by cloud architecture and cloud infrastructure. In this chapter, a theoretical foundation is built by reviewing the current literature to justify the research problem. As an outcome of this chapter, research opportunities that are not addressed by previous researchers and not exploited in practice are identified. This chapter has eight sections. Section 2.1 provides introduction to cloud computing. Chapter 2.2 provided strategy for literature review. Chapter 2.3 provide literature review on data privacy. Chapter 2.4 provides review on data security. Chapter 2.5 develops research problem. Chapter 2.6 provides summary of this chapter.

2.2 Literature review strategy

The objective of the literature review is to obtain a detailed understanding of the current state of knowledge surrounding cloud computing. The literature review strategy used in this research is based on the steps suggested by Higgins and Green (2006): (a) define the search terms; (b) identify databases and search engines and query using the search terms; (c) create and apply the inclusion and exclusion criteria filters; and (d) verify the selection is representative. A literature review protocol was developed after the definition of key search terms for the research subject area of cloud computing. A web search on the Google search engine was conducted for the keyword “Cloud Computing”. The search led to many results. Since Google presents search results based on relevance, the top 200 results were reviewed after which the results started to appear redundant and/ or irrelevant. Several web search results provided insight into the current market offerings, case studies, white papers, electronic articles, and reports about cloud computing.

2.2.1 Literature review protocol

Table 3: Literature review protocol

Search Terms	
Search Keyword combination	"Cloud Computing" **OR** “Data Privacy and Cloud Computing" **OR** "Data Security" "Cloud Governance" **OR** "Cloud Security" **OR** "Cloud Governance Framework" **OR** "IT Audit" **OR** "Network Security" **OR** "Computer Forensic"

General Search (online Databases and Search Engines)	
AIS Electronic Library	A central repository for research papers and journal articles relevant to the information systems academic community. http://aisel.aisnet.org/ (covers all major IS journals and AIS conference proceedings)
EBSCOhost Megafile Complete	Using EBSCOhost databases: 1. Academic Search Complete 2. Computers & Applied Sciences Complete 3. eBook Collection (EBSCOhost) Incorporating leading sources for academic journals from: a. ACM Portal b. IEEE Xplore c. Springer Link d. Decision Sciences e. Elsevier f. ScienceDirect g. Wiley InterScience
Google Scholar	Extensive repository of scholarly publications
Specific search (research outlets that have a focus on the area of process assessments)	
EuroSPI Proceedings	European System & Software Process Improvement and Innovation. Conference Repository http://www.eurospi.net/
SPICE Proceedings	Software Process Improvement and Capability Determination Conference Repository (in SpringerLink)
Standards On-Line Premium	Relevant ISO/IEC international standards
Search settings & selection criteria applied	
Language	English
Options	Scholarly (Peer reviewed) Publications, Full Text, References available
Date range	Jan 1980 to Dec 2020
Inclusion criteria	Papers on ITSM and process improvement/ process assessment that explain: 1. General concepts 2. General applications 3. Overall implementation issues 4. Overall improvement aspects 5. Quality process improvement concepts 6. Continual/ continuous service improvement

Search settings & selection criteria applied	
Exclusion Criteria	Papers on cloud computing that explain: 1. Specific cloud commuting functions 2. Specific applications of cloud computing 3. Specific applications of process managing cloud computing 4. Software improvement or software assessment for cloud computing

The literature review protocol is design to define scope of research while using online internet-based search engines, online databases, and electronic libraries. The literature review protocol describes the sources used to collect research paper and academic resources for review of literature. The ‘Search Keyword’ criteria is based on research title of this thesis and other directly & indirectly related academic areas. The inclusion criteria confirm that upon online search of the keyword all the possible information available is shown in search result. The exclusion criteria confirm to keep unrelated and irrelevant search result out of scope of literature review. Together, inclusion and exclusion criteria help to refine the search results from online databases.

2.3 Academic literature review on data privacy

Data privacy refers to appropriate use of data provided to corporations for agreed purposes (Coombs, K.A. 2005). Data collected by customers to meet the business requirements and need of customer should be sufficient, and it should be accepted by customer and with complete disclosure information being provided to them (Nwogu E., 2014). Federal Governments through regulators continues to impose penalty for not providing enough disclosure to customers and data privacy (Mell P., et. al., 2014). In Banking and Financial Services Industry, where data is collected to ensure identity of customer (Personally Identifiable Information – PII) (individual or corporations) (Chen et. al., 2014), to know the credit history, employment history, provide (or extend) credit facility, to manage life cycle of credit (loan), to develop analytical framework for future decision based on economic and financial markets – data privacy hold key to meet integrity of business and method to operate in competitive economy (Naydenov R. et. al., 2015). With this information of customers being available on cloud - data leakages, data theft, data tampering, data manipulation, data deletion (accidental or otherwise) - data privacy remains the key concern for Banking and Financial Services Industry (Hashizume K. et. al., 2013). Through this research, various data types critical for Banking Business operation and financial transaction available on cloud infrastructure will be evaluated and risk attached to them will be listed (Bisong A. et. al., 2011).

2.4 Academic literature review on data security

Data security refers to confidentiality, availability, and integrity of data (Boss & Kirsch, 2007). The data security means – it is accessible, used and processed by authorised users only (Zissis D. et. al., 2010). Data security ensures it is available, reliable, and accurate. Data security plan ensures collecting only required information, keeping it safe and destroying any information which is no longer needed (Sun Y. et. al., 2014). Data security plan helps businesses meet legal obligation of possessing sensitive data. In Banking and Financial Services Industry, the data is collected and evaluated on defined frequency to consistently remain adaptable to changing economy and business cycles (Mahalle et. al., 2018). This research will identify the challenges faced by Banks to provide the data security and system stability.

2.4.1 Systems Security

Systems security refers to its ability to protect information systems from external attacks (Deliberate or accidental) (Fisher E., 2016). Secured systems make them dependable and available when required, thus makes them reliable. Secured systems when operate as expected without failures and any delays helps achieve desired objectives for banking and financial services industry (Hashizume K. et. al., 2013).

Below are major security related concerns for Banking and Financial Services Corporations (Mahalle et. al., 2021):

1. Meeting governance and compliance requirements as per Banking and Financial Services industry standards to capture relevant personally identifiable information from customer and report complete information on timely basis.
2. User account control for both cloud services user and provider through identity and access management processes and systems

3. Contract negotiations and Service level agreements with cloud service providers considering round the clock availability and location of cloud service provider outside the geographical boundaries of Banking and Financial Services Corporations

4. Data confidentiality to protect customer’s and organizations information considering cloud support teams being located and accessing customer information remotely.

5. Data integrity to prevent data manipulation and deletion to confirm technical competency of cloud and application support team.

6. Cloud services availability considering Banking and Financial Services Operating across several nations and need low system outages.

7. Secure deletion of data once the data is used for investigation and fixes.

8. Malicious Insider considering several vendors having access to customer information.

9. Lack of transparency of the cloud services for application hosting and servers involved.

10. Data losses due to system or human errors due to oversight and lack of technical skills to handle data.

11. Data breaches due to lack of encryption and user awareness

12. User activity monitoring / visibility to keep log of user activities over cloud infrastructure.

13. Lack of forensic capabilities to investigate cases involving financial irregularities and fraud.

14. Loss of control over data due to cross border location cloud support teams and remote access

15. Lack of information in understanding of cloud security due to dual multiple security layers

16. Lack of clarity between cloud computing and outsourcing support

17. Lack of guidance on cloud adoption by industry and innovative ways to handle everyday incidents.
18. Requirements of current privacy and security certification schemes to meet regulatory requirements.

The above areas add risk to cloud security and requires constant audit and risk mitigation plans in place to secure cloud and provide uninterrupted services to customers and employees of Banking and Financial Services.

This research will identify areas of security breach incidents and area, system vulnerabilities, organization security policy that are required to provide robust framework for data privacy and security.

2.5 Development of research problem

The research problem that this research is motivated to solve has already been stated in Chapter 1. Addressing data privacy and system security are two major challenges of cloud computing. These challenges are considered as important problems that must be identified and solved by the proposed research. Based on the academic literature review and existing industry practices on data privacy and system security, the key problems of the additional risks of cloud computing architecture and cloud infrastructure are identified and justified next.

2.5.1 Need of additional processes for data privacy and system security

Cloud computing model and need of data privacy and system security demands additional processes to be completed to delivery of IT services to business users. With global delivery model and cloud services providers are spread across the globe, for an organization operating in Banking and Financial Services Industry, incorporating additional processes for data privacy and system security (Mahalle et. al., 2018). In competitive economic environment for an organization to organize and manage additional processes lead to additional tasks to be managed with additional human resources. These human resources demand further organization resources in the form of space and computing resources to complete these tasks (Uffen J. et. al., 2012). In this way, cloud computing adds additional processes and additional resource requirement (Talla M. et. al., 2013). This additional resource engagement adds new risk areas in the form of process risk and human involvement risk to data privacy and system security control framework.

2.5.2 Need of additional financial resources for data privacy and system security

As mentioned in above section 2.5.1 the need of human and organizational resources translates directly into need of financial resources for the organization. This put budgetary pressure on organization while securing data, data privacy and system security.

2.6 Chapter summary

This chapter provides details about the literature review strategy, method to seek literature and its use. This chapter details about data privacy, data security and system security related aspects of cloud computing. This chapter continues to define research problem and details its implication for organization in Banking and Financial Industry.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Chapter introduction

The objective of this chapter is to provide an explanation of the research activity plan in terms of philosophy, design and methods used during this research. The study is largely exploratory in nature, particularly during the artefact design and development. The choice of the research methods supports data collection that answers the research questions introduced in Chapter 1 and presented in the research model in Chapter 2. Chapter 4 and Chapter 5 provide further details about the actual design, development and evaluation of the data privacy and system security.

3.2 Research philosophy

Philosophy in business research is largely categorised by the researcher’s view of reality (ontology) and stance regarding valid knowledge (epistemology) (Saunders, Lewis & Thornhill 2009). This section discusses research philosophy to consider the ontology and epistemology positions of this research to direct the research methods used (Lee 2004). Garcia and Quek (1997) argued that as an applied discipline. IS research concentrates more on the outcomes and methodological issues. It should rather concentrate on ontological and epistemological reasoning behind a particular understanding of ontological, epistemological, and methodological concepts. The data privacy and system security provides a philosophical view within this research to articulate additional risk to cloud architecture and cloud infrastructure. Based on these inherent values, this research takes the philosophical worldview of critical realism (Bhaskar 1978) that guides the research design.

Below table 4 summarises how the philosophy of critical realism has driven the entire research process, along with the focus on the unit of analysis and the research questions.

3.3 Research design

Table 4: Research design

Research Philosophy	Critical Realism
Ontology	Realist view of world – a world exists independent of our knowledge, contrary to positivism which reduces the world for empirical measurement and many forms of constructivism which reduce the world to their knowledge of it (Mingers, Mutch & Willcocks 2013)
Epistemology	Different forms of knowledge exist – physical, social and conceptual – therefore a combination of different research methodologies is required
Research type	Exploratory Research
Research topic	Data privacy and system security for Cloud Architecture Infrastructure
Research problem	There is a risk associated with data privacy and system security on cloud computing architecture.
Research design	Quantitative Research Qualitative Research Case study research
Research approach	Phase 1. Literature review Phase 2. Research Survey Phase 3. Summative evaluation
Methods of data collection	Participatory Survey Questionnaire
Unit of analysis	"Quantitative Assessment" applied at "group level" (Data privacy and system security functions in an organization)
RQ1	What will be the impact to the various data categories and application types used by Banking and Financial Services Corporations due to cloud architecture and how it will impact the business and customers?
RQ2	What type of measures and controls will be required for cloud computing architecture for Banking and Financial Services Corporations to enforce data privacy and system security
RQ3	What will be the role of cyber security executives, security framework and governance structure to improve cloud security **of banking and financial services corporations**?
RQ4	What will be risks to customer data due to digital transformation in Banking and Financial Services Industry?
RQ5	How will cloud architecture support need of specific departments from bank for forensic investigation purposes **of banking and financial services corporations**?

3.4 Research methodology and analysis of data

3.4.1 The methodology chosen

A mix of qualitative and quantitative research methodology based on Case Study Method is followed for this research. As the research aims to identify data privacy and system security for Banking and Financial services Industry, a case study of bank is chosen to understand practical aspects of research. The case of a bank helps to relate theoretical research with practical application of research outcome. The research methodology explores and narrates the data privacy and system security related areas of cloud computing architecture with focus on Banking and Financial Services Industry. The research tries to interpret cloud computing for Banking and Financial Services Industry, data privacy and system security. The research has an exploratory approach to see various aspects of cloud computing.

To the support the findings of the research qualitative research in the forms of structured interviews and a questionnaire based quantitative data collection method is followed. The interview method is chosen to understand perception of cloud computing in terms of ease of use, complexity to connect, network security threat and technical support available to cloud computing users in bank. The survey method is chosen to assess of cloud architecture and cloud infrastructure on cloud governance and cloud security. The case study, interviews and survey aim to assess data privacy and system security of cloud computing architecture and cloud infrastructure for Banking and Financial Services Industry. The questionnaires have choice based objective answers for both survey and interviews.

3.4.2 Research design and data collection

As part of data collection strategy:

A. Data is collected from Research Papers and Journals published on cloud computing and cloud security for reviewing literature which is mentioned in research design in section 3.3 above.

B. Developing interpretation of reading relevant to Banking and Financial Services Industry is followed to derive importance of data privacy and system security.

C. Engaging in thought experiments and developing possible story lines considering different contexts of Cloud Computing relevant to Banking and Financial Services Industry

D. Naturalistic inquiry on available artefacts and studying real-world settings of cloud computing to interpret relevance to Banking and Financial Services Industry is followed.

3.4.2.1 Qualitative data - survey

According to Blackstone (2014), employing a survey method has several benefits. They are:

- Cost-effective as a survey enables to collect data from a representative sample size with a relatively low cost.
- Generalizable as a survey can be used for a relatively large sample and can provide a chance to collect abundant information from the respondents.
- Reliable as the survey questions are presented to respondents in a standard format with the exact same phrases; and
- Versatile as the respondents, particularly those in the large samples, come from different walks of life with different backgrounds. For this research sample with IT background was chosen to answer questionnaire appropriately

This also provides justification for the research approach.

Survey questionnaires are the primary data collection tool in this survey research. The first questionnaire explores factors such as data privacy and system security while operating on Cloud Computing Infrastructure. The second questionnaire measures the Bank’s concerns about data privacy and system security considering the existing challenges and effectiveness of cloud governance framework.

Both questionnaires contain three parts. In the first survey the first part will collect the demographic characteristics of the participants, including education, experience in IT, Experience in Banking and Financial Services Industry and experience to deal with Cloud Computing architecture and Infrastructure. The second part will question the respondent’s most recent experience with challenges of Cloud Computing

Infrastructure since its adoption. The third part of the survey will contain open questions to allow the respondent to make suggestions on improving the quality Cloud Computing Infrastructure, governing process and technology. This survey will help answer the questions of RQ1, RQ2, RQ3, RQ4 and RQ5.

The combinations of research questions and their answers was also included in questionnaires. This is covered in section 4.

3.4.2.2 Qualitative data - interview

The case of the major bank regionally established in Brisbane, Queensland, Australia and operating nationally, is selected as the cases to study. The theme of questionnaires derived by taking cloud governance framework, data privacy and system security aspects of this bank.

The structure of questionnaires was to present established architecture, tools techniques and methods; and question the risk, operational task, additional monitoring, change in mode operations, security policy implementation cloud architecture infrastructure has introduced for Banking and Financial Services Industry.

The interview was to evaluate over all perception and the experiences of Technology Leaders and IT Security experts with cloud computing architecture and infrastructure. The interviews conducted with Bank staff and IT Executives to determine way to improve the process and technology to protect the customers' information and improve security. These interviews will focus on the Bank IT Executives attitudes towards the Cloud Computing Infrastructure and the potential benefits.

The main topics of this round of interviews was:

- The importance of data privacy and system security; and
- The willingness to develop and adopt the Cloud Computing Infrastructure to ensure data privacy and system security.

A semi-structured interview used in this research because this research conforms to almost all of the following reasons/criteria mentioned in Whiting (2008): (1) Interview scheduled in advance at a designated time; (2) location normally outside everyday events and possibly after work hours; (3) organised around a set of predetermined questions based on area of cloud computing; (4) other questions and cross question emerge from dialogue; (4) usually interview will be planned for 30 minutes to 1 hour based on context of cloud computing.

Qualitative interviews are traditionally conducted on telephone (Novick, 2008; Qu & Dumay, 2011).

First, I had to consider the ethical and moral issues of the interview and establish a guideline for each stage of the interview. Various documents and literature were consulted, including the recent changes in architecture of Banking and Financial Services Industry, Industry publications, government bulletins and regulatory guidelines and research literature to develop the interview questions and follow-up probes. I had obtained approval from the University of Southern Queensland (USQ) for the ethics protocols before commencing the interviews.

Following information and data that was collected through the interviews:

The adoption of Cloud Computing Infrastructure in day-to-day operations:

- The impact of Cloud Computing Infrastructure on the Banks efficiency and profitability
- The impact on Privacy, security and governance of Bank
- The Bank’s plan for developing on premise IT Infrastructure (if any); and
- The factors that will continue to encourage Banks to continue using Cloud Computing Infrastructure

3.5 Data analysis and presentation

3.5.1 Qualitative data

Burnard et al. (2008) noted that there are two fundamental approaches to analysing qualitative data: the deductive approach and the inductive approach. The deductive approach involves using a predetermined framework to analyse the data while the inductive approach involves analysing the data with little or no predetermined theory, structure or framework. For this research, the inductive approach was, particularly the thematic content analysis which involves analysing answers provided in questionnaires and identifying themes within that data and gathering examples. The most important part of the analytical process is to identify, confirm and qualify the themes from the questionnaires.

Emery (2014) summarised six ways of displaying qualitative data visually: word clouds, showcasing open-ended survey data beside closed-ended data, photos beside a participant’s response, icons beside the descriptions and responses, diagrams to explain concepts and processes, and graphic timelines. In this research it is more appropriate to use answers provided in questionnaires for the quantitative interview data. This research adopted a confessional description approach with a focus on my own interpretations and analysis.

There are two major approaches to the presentation of the findings of the qualitative research (Burnad et al., 2018). One is simply to present the key findings under each main theme or category with verbatim quotes inserted to illustrate the findings. The other approach is also to present under each theme but also to incorporate the discussion into the findings. In this approach there is no need to have a discussion section. This approach was adopted for this research as there is a need to integrate the qualitative findings with the quantitative results to facilitate the discussion of ways to improve the data privacy and system security of cloud architecture infrastructure.

3.5.2 Quantitative data

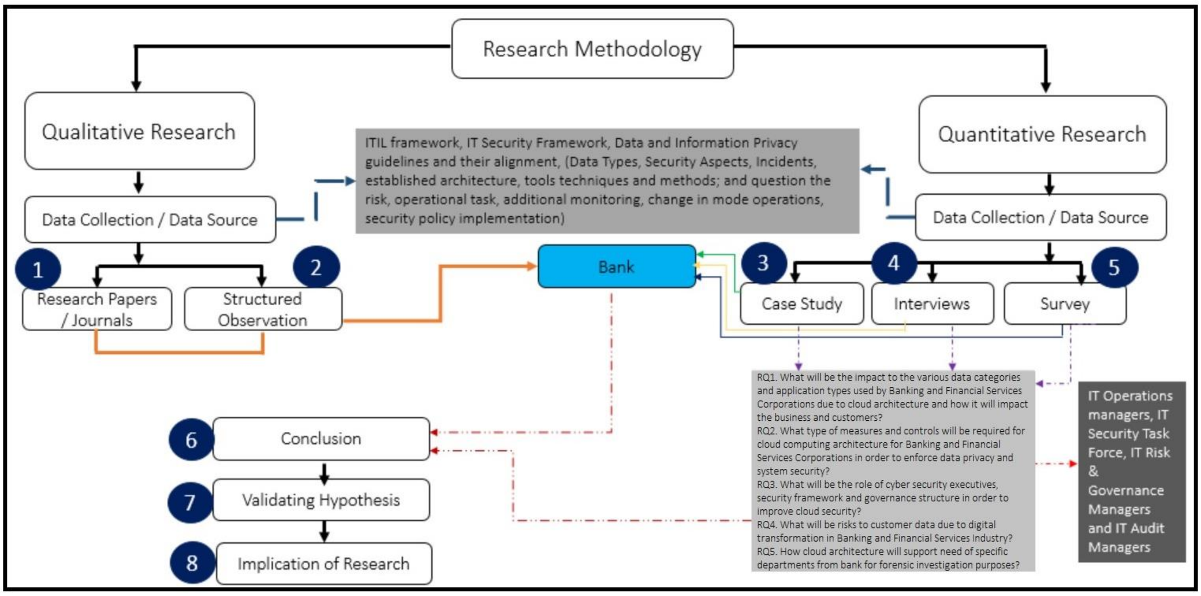
Factor analysis was used to identify the underlying dimensions of the data privacy and system security concerns. Principal component analysis and exploratory factor analysis collectively are often called factor analysis (Hutcheson & Sofroniou, 1999). They are both variable reduction techniques. However, the goal of exploratory factor analysis is to model a set of variables by latent factors that cannot be measured directly, while the goal of principal component analysis is to derive a relatively small number of variables that capture as much information as possible in the measured/observed variables (Leech, Barrett & Morgan, 2011). Exploratory factor analysis was appropriate in this research when the researcher’s goal is to identify a set of underlying common factors. Given that the factors determining privacy and security of the cloud architecture are adopted from the previous literature, it is more appropriate to use the principal component analysis approach. All the quantitative data in the survey is presented in both textual and visual (graphs and tables) forms in section 4 of this thesis. In this research the descriptive statistics, factor analysis and the cloud architecture results are be reported in tables.

3.6. Ethical considerations

This study will follow USQ's Ethical Guidelines strictly. All the interviewees and the participants of the survey were fully informed of the objectives of the research. The ethics clearance was obtained from USQ prior to conducting this survey and interview data collection. The data collected from the participants from the Bank and Financial Services Corporations was stored properly and used only for this research. No personal data or information was released to a third party without the permission of the participants. I had prepared all the ethics paperwork such as information sheets and consent forms carefully. I made it clear to all the participants that this paperwork is part of the normal routine for academic research. I had informed all the participants that their information will be kept confidential and that they have the right to withdraw from the research survey at any time.

3.7 Steps in research methodology

The following figure shows the research methodology:



Research Methodology
Qualitative Research
Quantitative Research
Data Collection / Data Source
Data Collection / Data Source
ITIL framework, IT Security Framework, Data and Information Privacy guidelines and their alignment, (Data Types, Security Aspects, Incidents, established architecture, tools techniques and methods; and question the risk, operational task, additional monitoring, change in mode operations, security policy implementation)
1
Research Papers / Journals
2
Structured Observation
Bank
3
Case Study
4
Interviews
5
Survey
RQ1. What will be the impact to the various data categories and application types used by Banking and Financial Services Corporations due to cloud architecture and how it will impact the business and customers?
RQ2. What type of measures and controls will be required for cloud computing architecture for Banking and Financial Services Corporations in order to enforce data privacy and system security?
RQ3. What will be the role of cyber security executives, security framework and governance structure in order to improve cloud security?
RQ4. What will be risks to customer data due to digital transformation in Banking and Financial Services Industry?
RQ5. How cloud architecture will support need of specific departments from bank for forensic investigation purposes?
IT Operations managers, IT Security Task Force, IT Risk & Governance Managers and IT Audit Managers
6
Conclusion
7
Validating Hypothesis
8
Implication of Research

Figure 1: Research methodology

Below are the steps followed in research methodology:

Step 1: Review literature to identify risk associated with Data and data Security for Cloud Computing Architecture. This step is theoretical information collection on data privacy and system security to identify risk in cloud infrastructure.

Step 2: Identify Data and Systems for Banking and Financial Services Corporations Cloud Computing Architecture. This step is to relate information collected in step 1 with Banking and Financial Services Industry in general. This step is also to relate information collected in step 1 and step 2 with case of a Bank.

Step 3: Based on Step 2 and 3 above, identify "risk parameters" and risk associated to data and Systems of Banking & Financial Services Corporations

Step 4: Take Case Study of a Bank

Step 4.1: Identify relevant stakeholders in Bank and with IT background.

Step 4.2: Schedule Interview based in topics identified as a part of research.

Step 5: Use Questionnaire to identify risk and risk mitigated steps Bank / stakeholders need to follow. The questionnaire has 43 questions which are linked to 5 research questions of this research. The grouping of survey questions and linking to research questions is detailed in section 4 of this thesis.

Step 5.1: The Survey used the dedicated technology platform provided by 3rd party company.

Step 5.2: Use Survey tool to design and mail questionnaire.

Step 6: Based on Step 5 and Step 6, conclude / summarise the findings of Questionnaire.

Step 7: Validate Hypothesis based results obtained in step 6 above.

Step 8: Summarise implications of the research.

The above steps confirm to provide all the information required to collect qualitative and qualitative data for the research study.

Summary of research methodology:

Data collection (step 1 – 2) → Develop Questionnaires (Step 3) → Identify research participants (step 4 – 4.1) → Conduct Interview (step 4.2) → Email survey questionnaire (step 5 – 5.2) → Summarise Findings (step 6) → Link Findings with Research questions (step 7) → Conclude (step 8)

3.8 Participants in interview and survey

Number of Participants in Interview and Method of selection: Sampling Methodology:

As a part of this research, the interview will involve 205 participants.

Criteria for Sampling 205 Participants:

1. Brief educational background
2. Experience in IT
3. Technology understanding and work on cloud environment.
4. Knowledge and Experience of working on Cloud Architecture.
5. Ability to answer interview questions.
6. Belonging to diversified areas of cloud infrastructure
7. Availability for interview, direct or indirect relation to Interviewer
8. Relevant work and experience on Cloud Infrastructure
9. Engagement in associated areas to govern cloud infrastructure and Operational understanding to manage cloud infrastructure.

The research also collected participants perception in interview questionnaires as well in terms of their –

1. Ease of use
2. Flexibility to work (WFH)
3. Data confidentiality and information security maintenance
4. Simplicity to connect to cloud architecture infrastructure.
5. Availability of all computing resources over cloud architecture infrastructure
6. Secure to connect from private network to cloud architecture infrastructure.
7. Ability to recover data in case of loss from cloud architecture infrastructure.
8. IT Support from remotely located teams in case of incidents raised for issue with cloud architecture infrastructure.

3.8.1 Total population of potential participants

Total population of IT Department with Banking & Financial Service and technology background is approx. 205. This includes as all people working in IT Department (Full time, part time, and casual employees, with knowledge of Cloud Architecture)

3.8.2 Criteria used to arrive at 205 participants

These 205 participants work on different set of areas on Cloud Infrastructure (Details of the Participant Background is given in section 4 of the thesis). These participants are aware of academic pursuit of PhD and will support to complete interview. These 205 participants were available for interview questionnaire as well.

3.9 Demonstration of no coercion, that participation or non-participation is anonymous

To meet this condition, the research followed ethical. The sample size for the survey were employees of the Bank and other participants were with experience in IT. I had reached them through online survey tools provided by 3rd party vendor.

Participation rate for survey and Interview was 100%, so all 205 people participated in survey.

3.10 Chapter summary

This research is a field study in IS driven by the motivation to develop and evaluate a novel method. The guiding principles of quantitative research methods, qualitative research methods and case study research are used to structure the research design. The goal of this research is to produce a research additional risk to data privacy and system security introduced by cloud computing architecture and infrastructure. The research will improve the current environment cloud computing by facilitating the application of research findings. Therefore, a quantitative research method, qualitative research methods and case study research methodology is suitable for this research. The environment within which this research project is conducted is an IT organization where a novel method to managed cloud computing architecture and infrastructure is practiced. Questionnaire methods is used to collect data. Based on the detailed explanation of the research methodology in this chapter, the thesis can proceed with a description of the research artefact, Chapter 4.

CHAPTER 4: DISCUSSION

4.1 Chapter introduction

This chapter summarises and interprets the findings from the survey questionnaires and the evaluation of the questionnaires mentioned in Chapter 3. The aim of this chapter is to discuss the findings in terms of each of the five research questions. This chapter provides context and meaning to the study by raising several discussion points for each research question following the research principles of abstraction, originality, justification, and benefit (Österle et al. 2011).

The summary and interpretation in this chapter are provided within the context of the study findings from chapters 3 and prior research findings reviewed in Chapter 2. While chapters 3 reported the results of the research activities during questionnaire development and sampling, this chapter lays emphasis on the interpretation and importance of the findings to articulate key discussion areas that impact research and practice. This chapter brings the research objectives and activities together to discuss the findings of the research questions along with the reflection on research work conducted and the prominent themes emerging from each research question.

In this chapter *section 4.2 to 4.3* focus on findings for the research questions.

4.2 Context of research discussion

This research used a survey to identify additional risk to data privacy and system security to cloud architecture an interpretative case study research to evaluate the usability survey findings. Discussions emergent from the research methods and outcomes reported in this chapters provide a context to communicate the impacts that this research can make. Chapters 1, 2 and 3 provided justification of the research problem, research opportunities and the research method simultaneously. The findings of the five research questions were presented in chapters 1. This chapter focuses on the discussions about the five research questions.

Table 5: Discussion section of thesis chapter 1-4

Thesis chapter	Chapter focus	Discussion context	Discussion section
Chapter 1. Introduction	Introduction of research questions	Justification of the research problem leading to research questions	Chapter 1, section 1.3
Chapter 2. Literature Review	Research model	Development of research opportunities	Chapter 2, section 2.5
Chapter 3. Research Methodology	Research plan	Justification of planned research activities	Chapter 3, section 3.3 to 3.6
Chapter 4 Survey Evaluation	Activity relating to evaluation of survey	Discussion of findings for RQ1 to RQ4	Chapter 4, sections 4.2 to 4.7

4.2.1 Survey participant details

Table 6 shows 134 participants and Figure 2 shows 65% of the survey participants have Full-time.

Table 6: Employment type of survey participants

What is your current employment status?		
Type of Employment	**No. of Employee**	**No. of Employee as % of Total**
Self Employed	57	27.80%
Full-time	134	65.37%
Part-time	12	5.85%
Casual	1	0.49%
Student - working casual /part-time	0	0.00%
Student - working full time	1	0.49%
Student - not working	0	0.00%
Retired	0	0.00%
Unemployed	0	0.00%
Home Duties	0	0.00%
Pension	0	0.00%
Other	0	0.00%
Total	**205**	**100.00%**

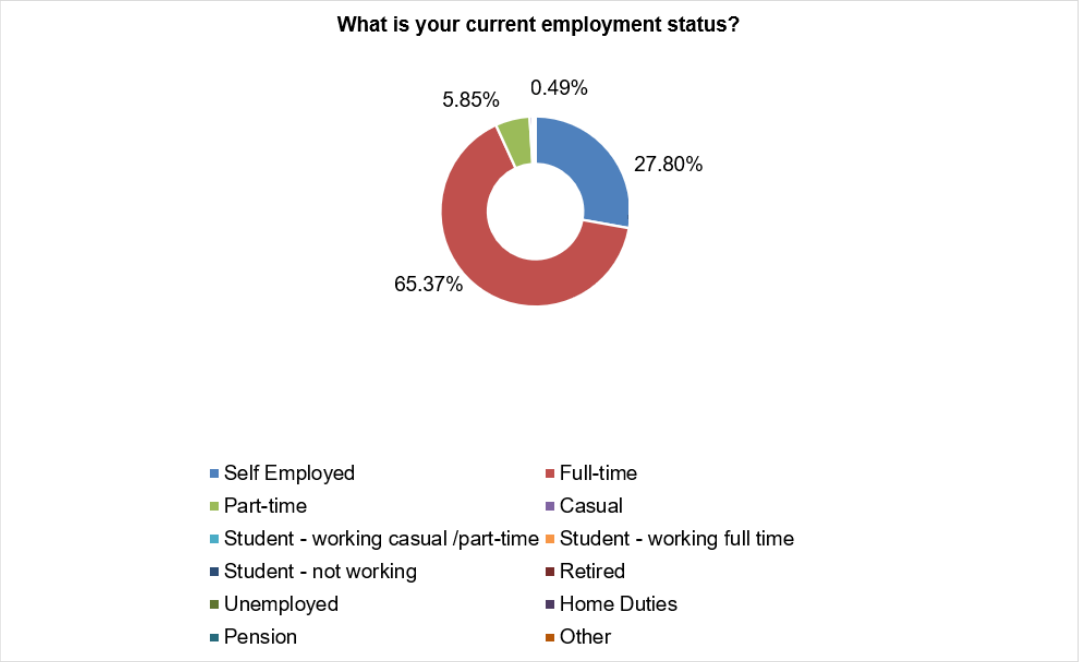


Figure 2

4.2.2 Industry type of survey participants

Table 7 shows 205 participants and Figure 3 shows percentage of survey participants.

Table 7: Industry type of survey participants

Which of the following best describes the industry you work in?		
Type of Industry	**No. of Employee**	**No. of Employee as % of Total**
Agriculture/Farming/Forestry/Conservation	4	1.95%
Arts/Culture	1	0.49%
Banking Business Services (Consulting & Strategy/Coaching/ Human Resources)	25	12.20%
Charities/Not-for-profit/Religious/Community Services	5	2.44%
Construction/trades	14	6.83%
Education & Training	13	6.34%
Engineering/Architecture/ Design	5	2.44%
Banking and Financial services/Insurances	22	10.73%
Government & Defence	5	2.44%
Health Services/Medical/Carers	8	3.90%
Hospitality/Accommodation/Food Services/Entertainment	5	2.44%
Bank Information & Communication Technology	49	23.90%
Innovation, Science & Technology	3	1.46%
Legal	2	0.98%
Manufacturing	8	3.90%
Marketing/Media/Advertising/PR	0	0.00%
Mining, Resources & Energy	1	0.49%
Real Estate & Property	4	1.95%
Retail & Consumer products	8	3.90%
Sport & Recreation	2	0.98%
Tourism	1	0.49%
Transport & Logistics	6	2.93%
Utilities: Electricity/Gas/Water/Waste	0	0.00%
Wholesale	5	2.44%
Other industry	9	4.39%
Prefer not to say	0	0.00%
Total	**205**	**100.00%**

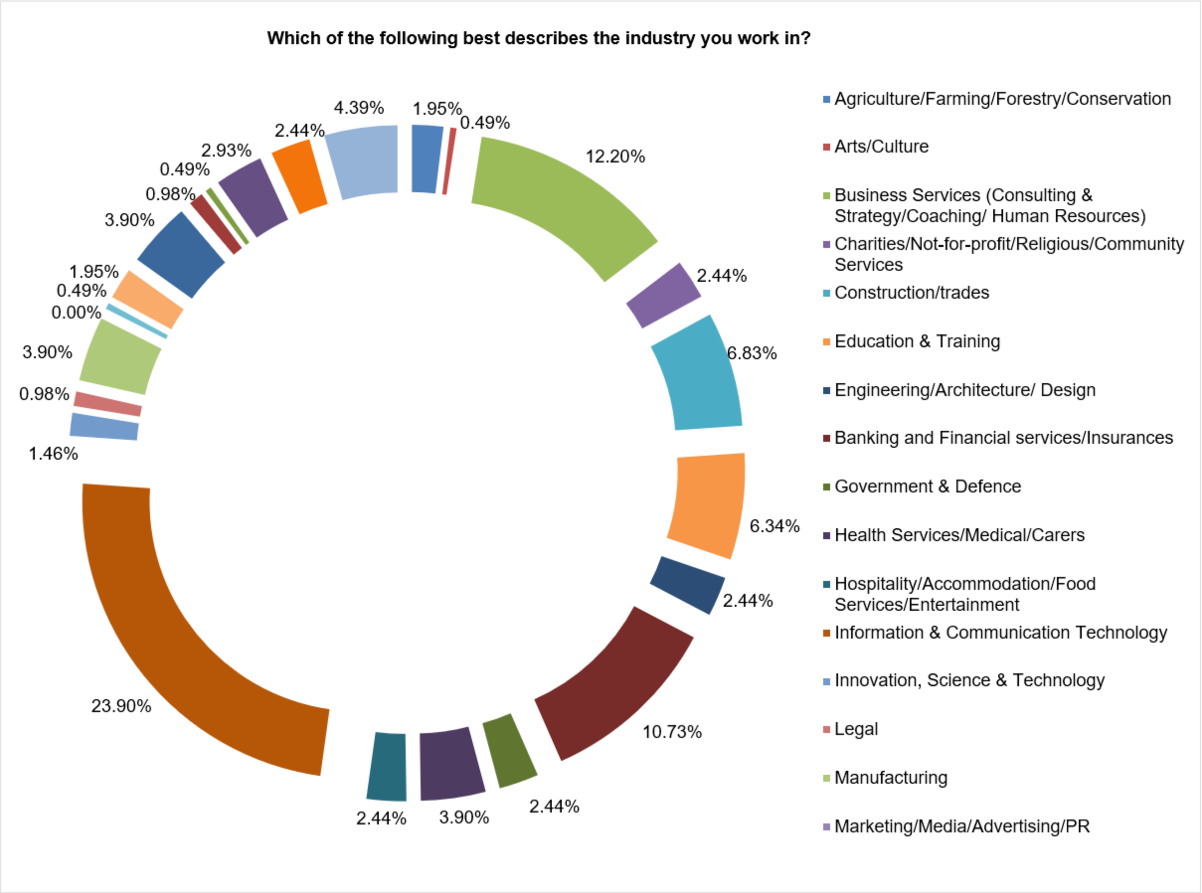

Which of the following best describes the industry you work in?
4.39%
1.95%
0.49%
12.20%
2.44%
6.83%
6.34%
2.44%
10.73%
2.44%
3.90%
2.44%
23.90%
1.46%
0.98%
3.90%
0.00%
0.49%
1.95%
3.90%
0.98%
0.49%
2.93%
2.44%
Agriculture/Farming/Forestry/Conservation
Arts/Culture
Business Services (Consulting & Strategy/Coaching/ Human Resources)
Charities/Not-for-profit/Religious/Community Services
Construction/trades
Education & Training
Engineering/Architecture/ Design
Banking and Financial services/Insurances
Government & Defence
Health Services/Medical/Carers
Hospitality/Accommodation/Food Services/Entertainment
Information & Communication Technology
Innovation, Science & Technology
Legal
Manufacturing
Marketing/Media/Advertising/PR

Figure 3

4.2.3 Information Technology (IT) work areas of survey participants

Table 8 shows 151 survey participants from work profile in IT operations and Figure 4 shows 73.66% of survey participants from IT operations.

(In this question, people have selected more than one option while answering, so the number of responses is more than 205. Example: Out of 205 survey responses, 129 participants have one of the work responsibility/profiles in 'IT security'

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 8: IT work areas of survey participants

Are you responsible for any of the following activities at your place of work?		
IT work Area	**No. of Employee**	**No. of Employee as % of Total**
IT security	129	62.93%
IT Audit	74	36.10%
IT operations	151	73.66%
IT risk management	108	52.68%
IT Governance and policy design	93	45.37%
Other IT - please specify	18	8.78%
None of the above	0	0.00%

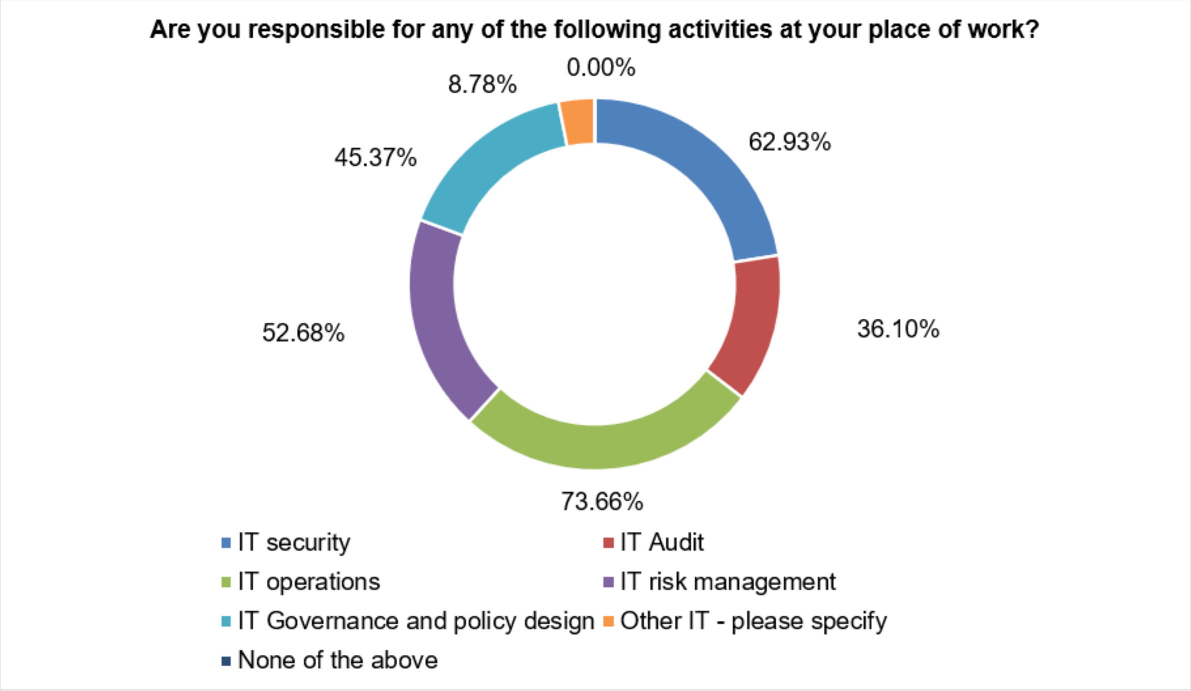


Figure 4

4.2.4 IT work experience of survey participants

Table 9 show that in survey, for 40 participants each has 3-5 years & 7-10 years of IT work experience and Figure 5 shows 19.51% relevant IT work experience for above mentioned work experience.

Table 9: IT work experience in years

How long have you been working in your current role at your place of work?		
Duration	**No. of Employees**	**No. of Employee as % of Total**
Under 3 years	33	16.10%
3-5 years	40	19.51%
5-7 years	31	15.12%
7-10 yeas	40	19.51%
10-15 years	33	16.10%
Over 15 years	28	13.66%
Total	**205**	**100.00%**

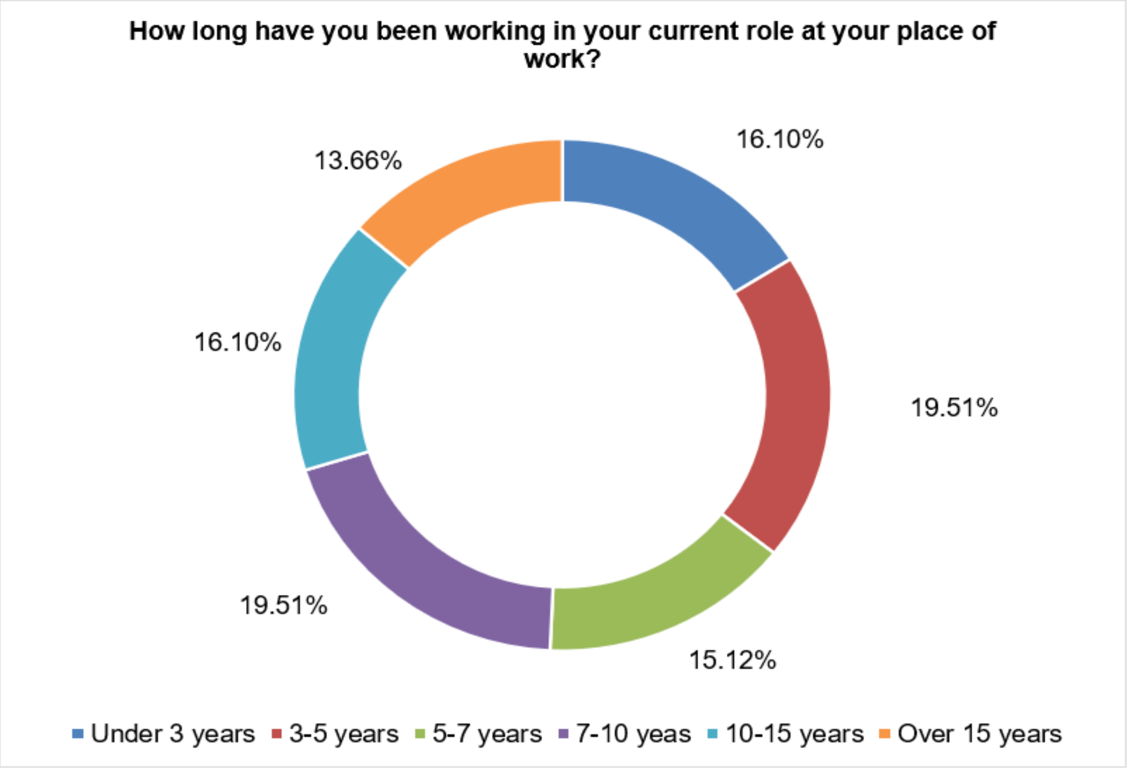


Figure 5

4.2.5 Relevant Work Experience in data privacy and system security in an organization

Table 10 shows that 205 survey participants and Figure 6 shows that 100% of survey participants have work experience in data privacy and system security.

Table 10: Work experience in data privacy and system security

Can you confirm as a part of your role in the business that you look after aspects around data and IT management, governance, infrastructure, and security?		
Response	**No. of Employee**	**No. of Employee as % of Total**
Yes	205	100.00%
No	0	0.00%
Total	**205**	**100.00%**

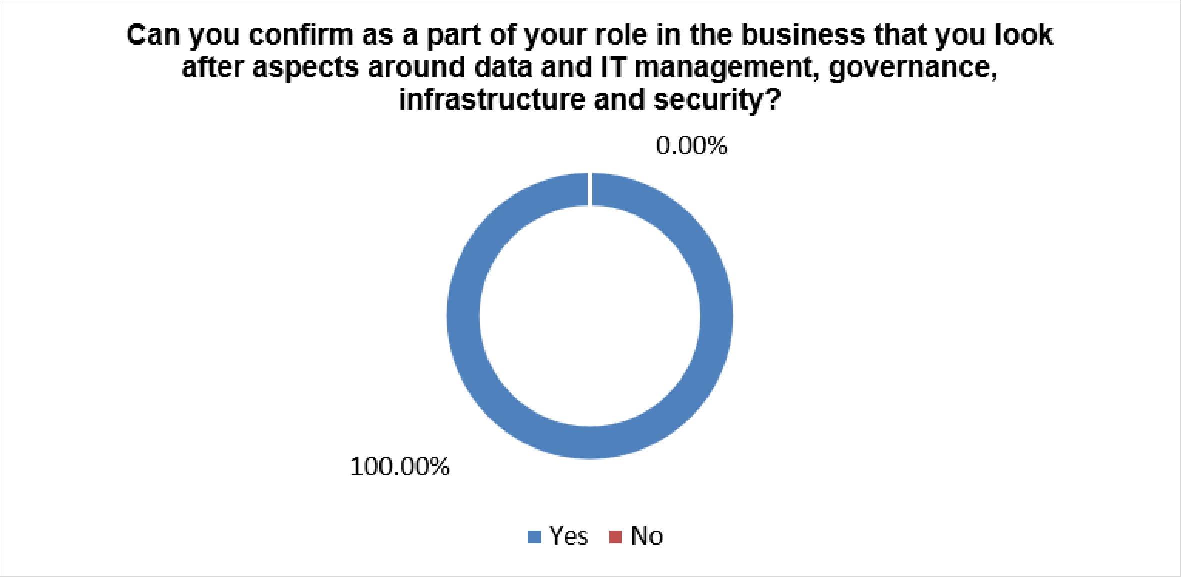


Figure 6

The above data captured as a part of survey participants confirms relevance of the participants for the survey.

Table 11 and Figure 7 shows number of survey questions linked to research question. Survey questions are linked to more than one research question. Example: Research Question 1 (RQ1) have 13 questions in survey questionnaire

Table 11: Below table shows research questions organization and summary.

Research Question (RQ)	No. of Survey Questions
RQ1	13
RQ2	25
RQ1 and RQ2	22
RQ3	3
RQ1, RQ2 and RQ3	7
RQ4	3
RQ1, RQ2 and RQ4	6
RQ1, RQ2, RQ3 and RQ4	6
RQ2 and RQ4	2
RQ5	2
RQ1, RQ2, RQ3, RQ4 and RQ5	1
RQ1, RQ2, RQ4 and RQ5	1
RQ1, RQ2 and RQ5	1

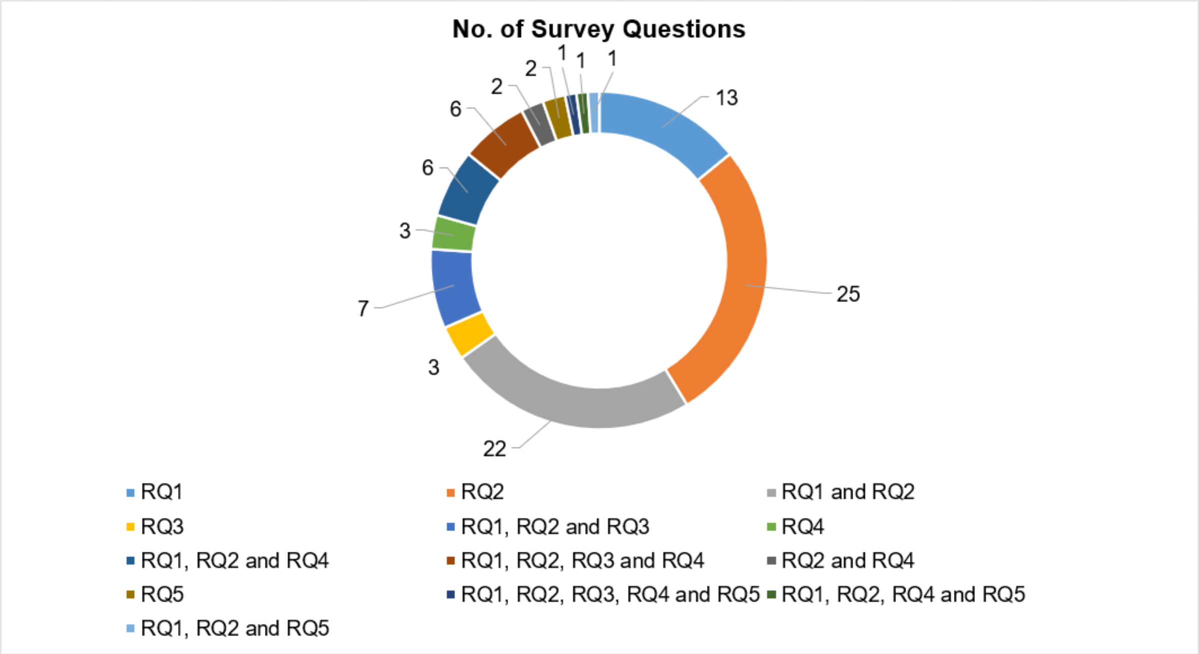


Figure 7

4.2.6 Discussion of research question 1 (RQ1)

RQ1 is a research question that asked how cloud computing model will impact data privacy and system security to banking and financial services corporation? This section 4.2.1 provides detailed questions for RQ1 and feedback received by survey participants.

Table 12: Below table shows linking of RQ1 with 13 survey questions.

Question No. in questionnaire	Question Description	Research Question No.	Research Area
2	Who are accountable people for cloud governance?	RQ1	Cloud Governance
4	What is area of re-design for cloud improvements?	RQ1	Cloud Governance
5	What are key parameters of Cloud Score Card / Cloud Operational Excellence?	RQ1	Cloud Governance
6	What are areas of cloud computing that confirms the value delivery to business?	RQ1	Cloud Governance
7	What are areas of Cloud improvement investment?	RQ1	Cloud Governance
8	How data categorization over cloud and its governance is related?	RQ1	Cloud Governance
14	How is cloud maturity model evaluated with change in architecture?	RQ1	Cloud Governance
18	On the scale of 1 to 10 (1 being lowest and 10 being highest) will you rate effectiveness of cloud governance for cloud operability?	RQ1	Cloud Governance
25	Does enterprise information architecture model support creation, use and sharing of data by users in a way to maintain integrity and is secure from failures?	RQ1	Cloud Governance
1	What is most important area in IT security implementation?	RQ1	Cloud Security
2	What are most important areas of security breach incidents related to data?	RQ1	Cloud Security
3	What are security perimeter controls to monitor data leakages?	RQ1	Cloud Security
23	Do you define the encryption methods based on data type?	RQ1	Cloud Security

The column “Question No.” in above table shows the sequence number in actual questionnaire emailed to participants.

Below list of tables (Table 13 – Table 25) shows the responses received for Research Question 1 (RQ1) from survey Participant.

Table 13 shows that 103 of the total survey participants responded that cloud is governed by IT operations teams in organization and Figure 8 shows that 50.24% of cloud is governed by IT operations teams in an organization.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 13: IT department to support infrastructure governance (cloud) framework.

Who monitors, maintain, and supports (accountable) IT infrastructure (Cloud) governance?		
Department	**No. of Responses**	**No. of Responses as % of Total**
IT Operations	103	50.24%
IT Security	85	41.46%
IT Risk Management	68	33.17%
IT Management and CIO Office	67	32.68%
Executive Team in company / Bank including Banking and Risk Management	40	19.51%
Others [3rd Party IT Management Teams]	40	19.51%

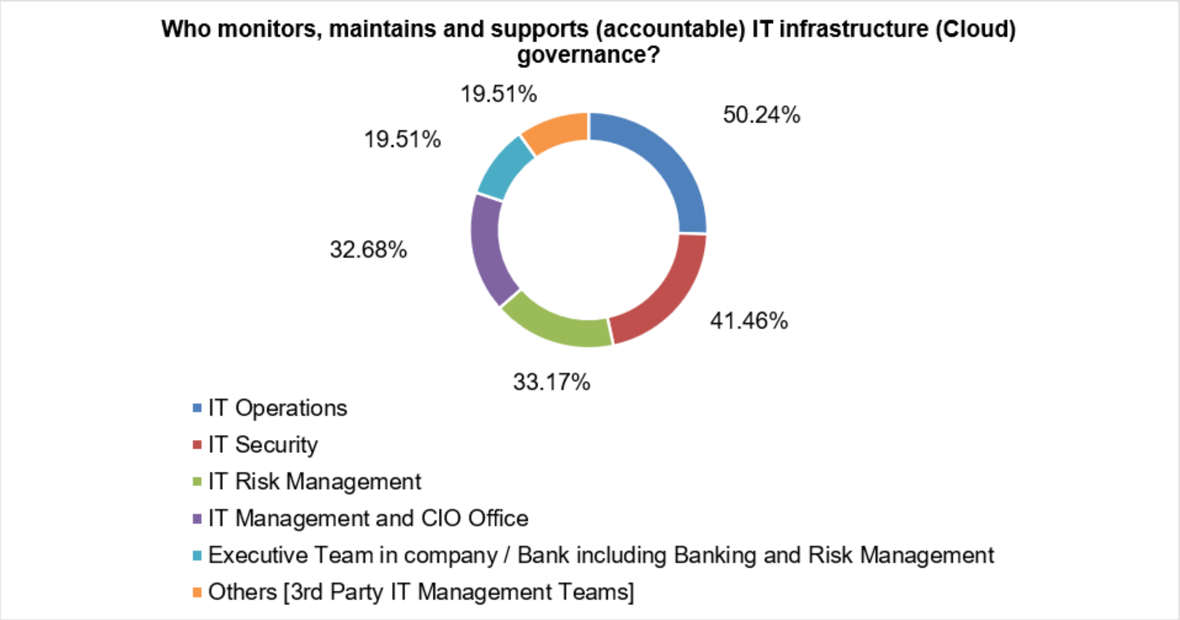


Figure 8

Table 14 shows that 115 of the total participants responded that 'IT infrastructure Security' requires re-design for IT infrastructure (Cloud) improvement and Figure 9 shows that 56.10% of participants responded that 'IT infrastructure Security' requires re-design for IT infrastructure (Cloud) improvement.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 14: Areas of re-design for IT infrastructure (cloud) improvements

What are areas of re-design for IT infrastructure (Cloud) improvements for the business/company? This refers to various departments in Company to manage cloud / IT devices and software		
Area	**No. of Responses**	**No. of Responses as % of Total**
IT infrastructure Operations	96	46.83%
IT infrastructure Security	115	56.10%
IT infrastructure Audit	69	33.66%
IT infrastructure Risk Management	87	42.44%
IT infrastructure Network	79	38.54%
IT Hardware Infrastructure (Routers, Switches, Server, Virtual Machines)	84	40.98%
None	18	8.78%
Unsure	11	5.37%

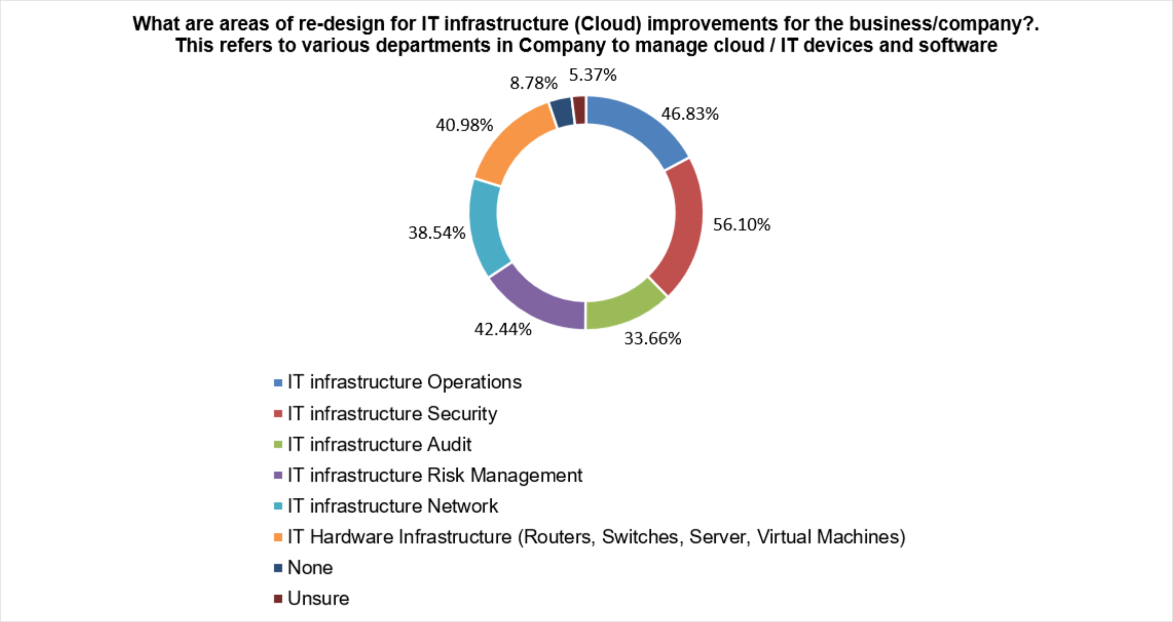


Figure 9

Table 15 shows that 116 of the total survey participants responded that ‘Response to high priority / critical incidents' form part of IT operational excellence and Figure 10 shows that 56.59% of participants responded that ‘Response to high priority / critical incidents' form part of IT operational excellence.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table15: Key parameters for IT infrastructure score card

What are the key parameters for IT infrastructure Score Card(s) / IT Operational Excellence?		
Parameters	**No. of Responses**	**No. of Responses as % of Total**
Number of high priority / critical Incidents	116	56.59%
Number of technical changes over IT infrastructure	101	49.27%
Number of Security breach Incident	114	55.61%
Number of Audit Findings	83	40.49%
Number of vulnerabilities identified and not mitigated	87	42.44%
Unsure / don't know	22	10.73%

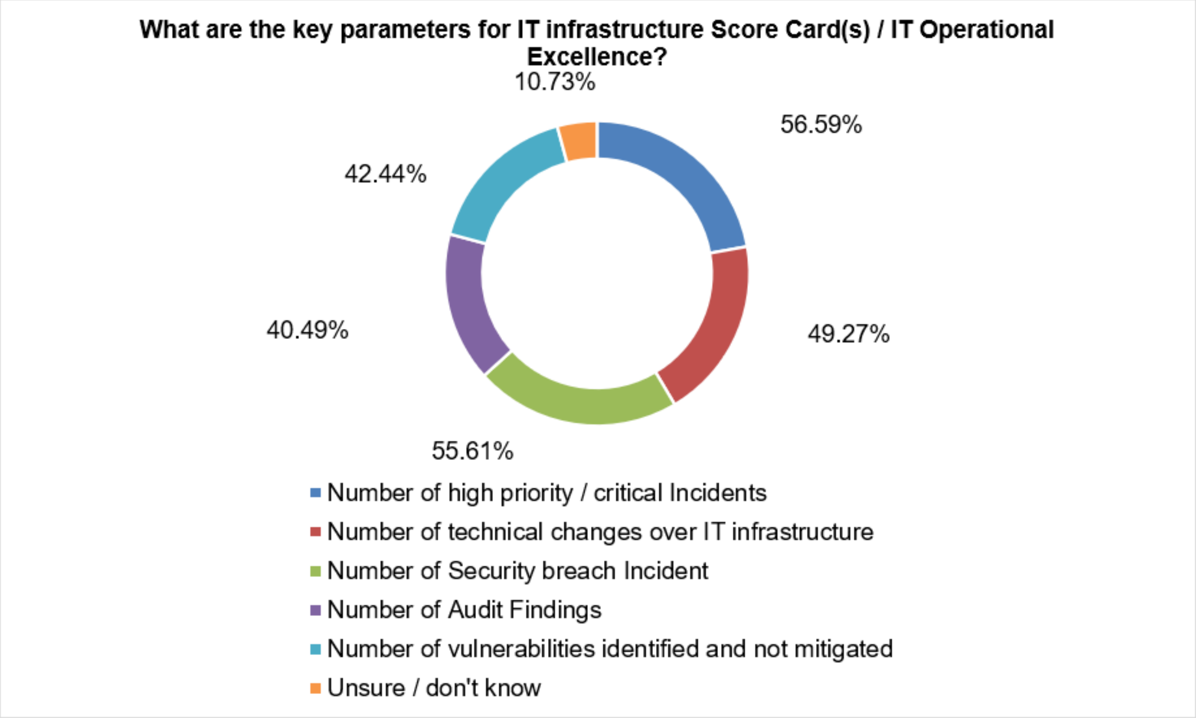


Figure 10

Table 16 shows that 92 of the total survey participants and Figure 11 shows that 44.88% of the total survey participants responded that ‘Application availability over IT infrastructure (cloud) platform, Customer Feedback for application over IT infrastructure (Cloud) Platform, IT infrastructure (cloud) Availability, IT infrastructure (Cloud) Accessibility, IT infrastructure (Cloud) Security' together are important for value delivery for business systems.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 16: Value delivery of cloud infrastructure

What are areas of IT infrastructure (Cloud) computing, that confirm the value delivery of the business?		
Areas	**No. of Responses**	**No. of Responses as % of Total**
Application availability over IT infrastructure (cloud) platform	76	37.07%
Customer Feedback for application over IT infrastructure (Cloud) Platform	51	24.88%
IT infrastructure (cloud) Availability	87	42.44%
IT infrastructure (Cloud) Accessibility	83	40.49%
IT infrastructure (Cloud) Security	66	32.20%
Combination of All of above (mention A, B, C etc.)	92	44.88%

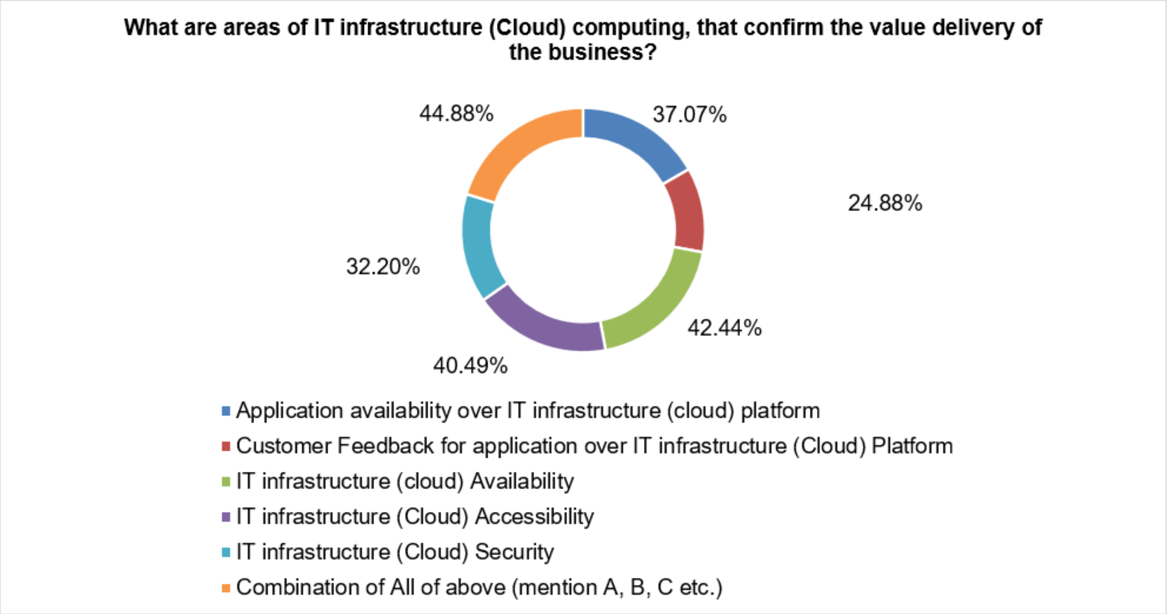


Figure 11

Table 17 shows that 123 of the total survey participants and Figure 12 shows that 60.00% of participants responded that ‘Application availability over IT infrastructure (cloud) platform, Customer Feedback for application over IT infrastructure (Cloud) Platform, IT infrastructure (cloud) Availability, IT infrastructure (Cloud) Accessibility, IT infrastructure (Cloud) Security' together are important for value delivery for business systems.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 17: Areas of IT infrastructure (cloud), improvement investments

What are areas of IT infrastructure (Cloud), improvement investments for the business?		
Areas	**No. of Responses**	**No. of Responses as % of Total**
IT infrastructure (Cloud) Security	120	58.54%
IT infrastructure (Cloud) (Hardware)	96	46.83%
IT infrastructure (Cloud) (Software)	123	60.00%
IT infrastructure (Cloud) Incident and problem management Services (ITIL)	89	43.41%
IT infrastructure (Cloud) Audit	52	25.37%
IT infrastructure (Cloud) Risk Management	71	34.63%

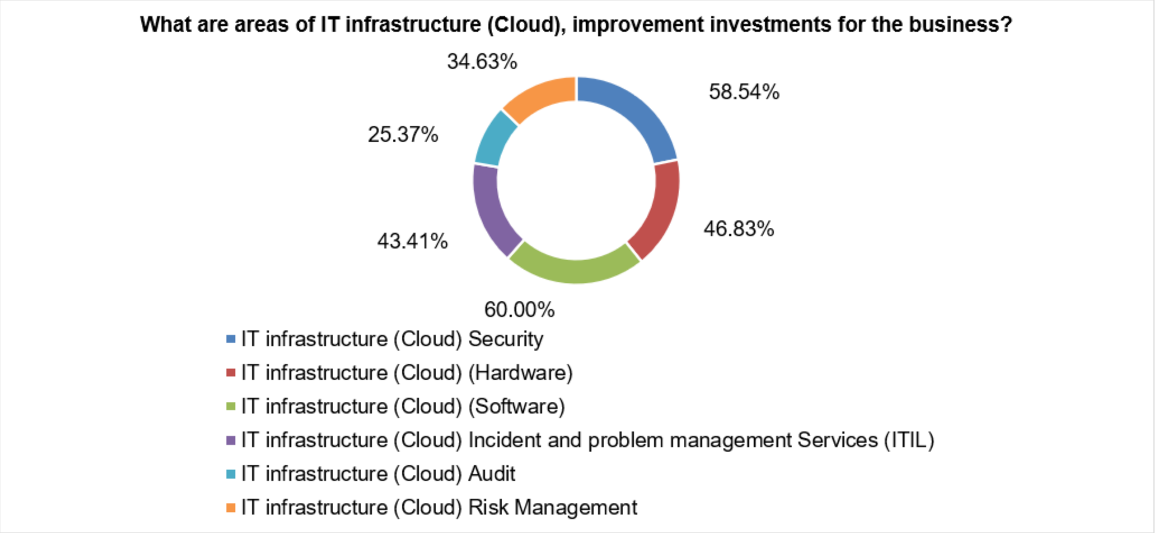


Figure 12

Table 18 shows that 130 of the total survey participants and Figure 13 shows that 63.41% of participants responded that 'Personal data', followed by 'Client/Customer account data history' are major 'Data categorization' areas.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 18: Data categorizations and relation to IT infrastructure (cloud) governance

How are data categorizations related to IT infrastructure (cloud) and its governance?		
Data Category	**No. of Responses**	**No. of Responses as % of Total**
Personal Data	130	63.41%
Credit Card Data	79	38.54%
Client / Customer Account Data History	129	62.93%
Software / Application Configuration Data	98	47.80%
Hardware Set up / Configuration Data	71	34.63%
Internal company / Office / Corporate Data	91	44.39%
Internal Finance and Planning Data	73	35.61%
Confidential, Secret, Private, Public Data only	80	39.02%

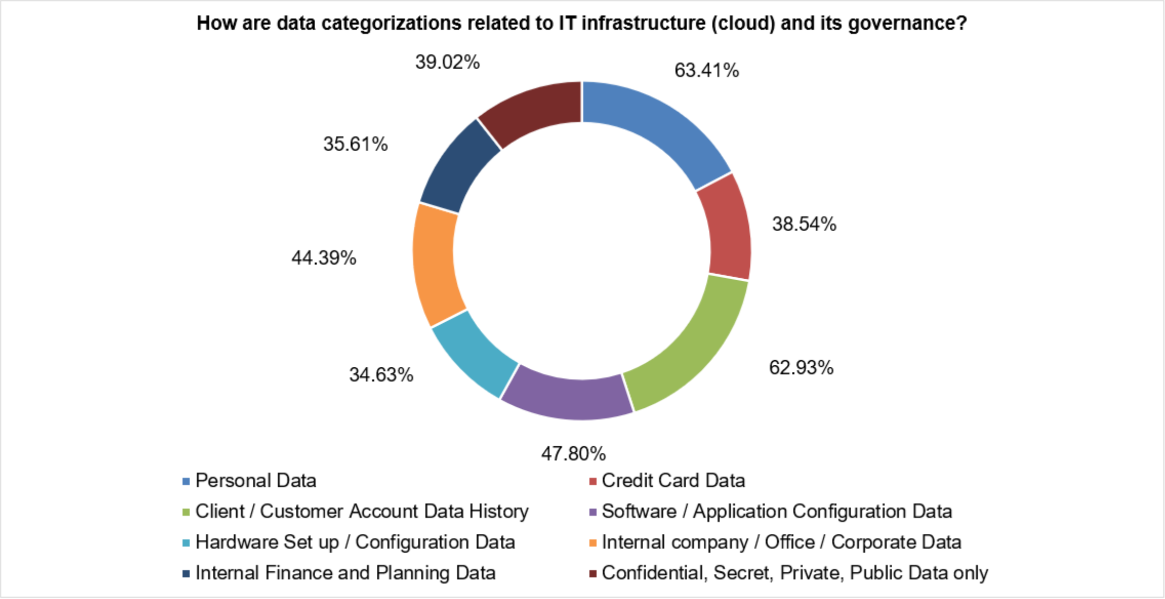


Figure 13

Table 19 shows that 136 of the total survey participants and Figure 14 shows that 66.34% of participants responded that ‘Ongoing Project Planning Phase includes development of maturity model (completeness definition)’ is most important to assess IT infrastructure (Cloud) maturity model (completeness)

Table 19: IT infrastructure (Cloud) maturity model (completeness)

How is IT infrastructure (Cloud) maturity model (completeness) evaluated with change to the IT architecture?		
Maturity Model Evaluation	**No. of Responses**	**No. of Responses as % of Total**
IT meeting with changing IT infrastructure (Cloud)	110	53.66%
Ongoing Project Planning Phase includes development of maturity model (completeness definition)	136	66.34%
One Time Quarterly Planning defines IT infrastructure (Cloud) maturity model	46	22.44%
Others (specify)	6	2.93%
Total	**205**	**100.00%**

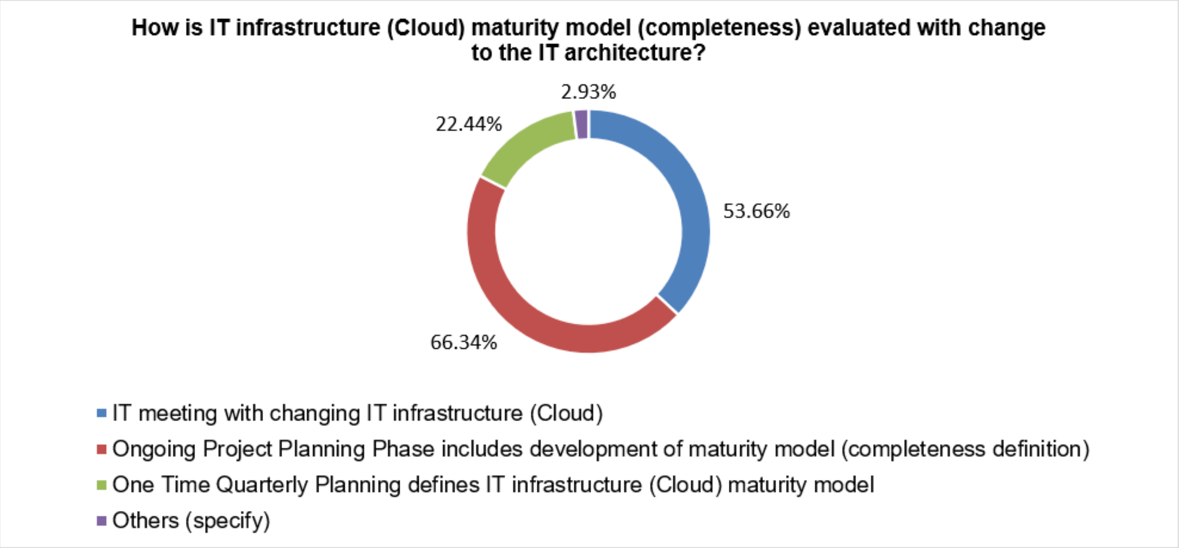


Figure 14

Table 20 shows that 116 of the total survey participants and Figure 15 shows that 56.58% of participants responded that ‘effectiveness of IT infrastructure (Cloud) management / governance for cloud operability’ is highly effective (rating 7 and 8)

Table 20: Rating scale for effectiveness of IT infrastructure

On the scale of 1 to 10 (1 being lowest and 10 being highest) how do you rate effectiveness of IT infrastructure (Cloud) management / governance for cloud operability?		
Scale	**Rating Responses**	**No. of Responses as % of Total**
1	0	0.00%
2	2	0.98%
3	3	1.46%
4	4	1.95%
5	13	6.34%
6	22	10.73%
7	58	28.29%
8	58	28.29%
9	26	12.68%
10	19	9.27%
Total	**205**	**100.00%**

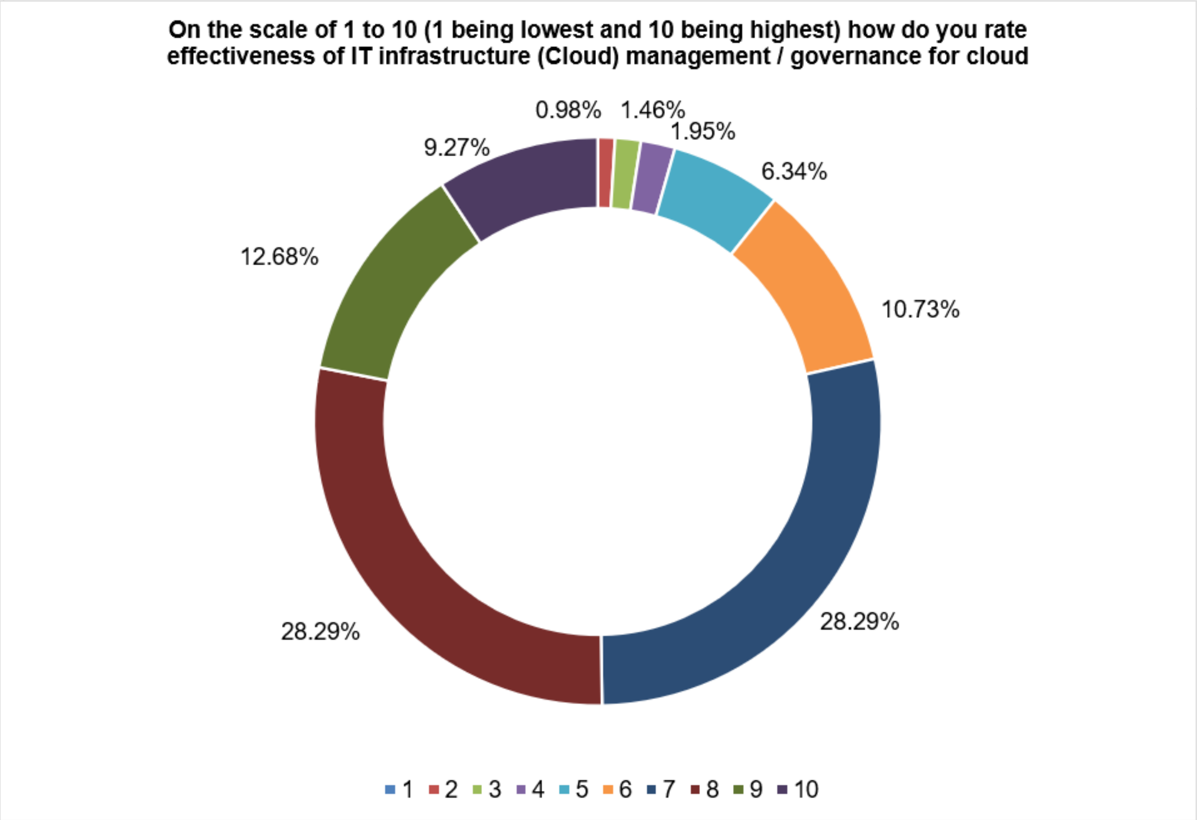


Figure 15

Table 21 shows that 112 of the total survey participants and Figure 16 shows that 54.63% of participants responded that ‘company / enterprise information architecture model support, creation, use and sharing of data by users in a way to maintain integrity and is secure from failures.

Table 21: Use and sharing of data over IT infrastructure.

Does company / enterprise information architecture model support, creation, use and sharing of data by users in a way to maintain integrity and is secure from failures?		
Scale	**No. of Responses**	**No. of Responses as % of Total**
Yes – Information architecture clearly supports data integrity, its use and sharing	112	54.63%
No – Information architecture loosely supports data integrity	54	26.34%
No – None of above	17	8.29%
Unsure / don't know	22	10.73%
Total	**205**	**100.00%**

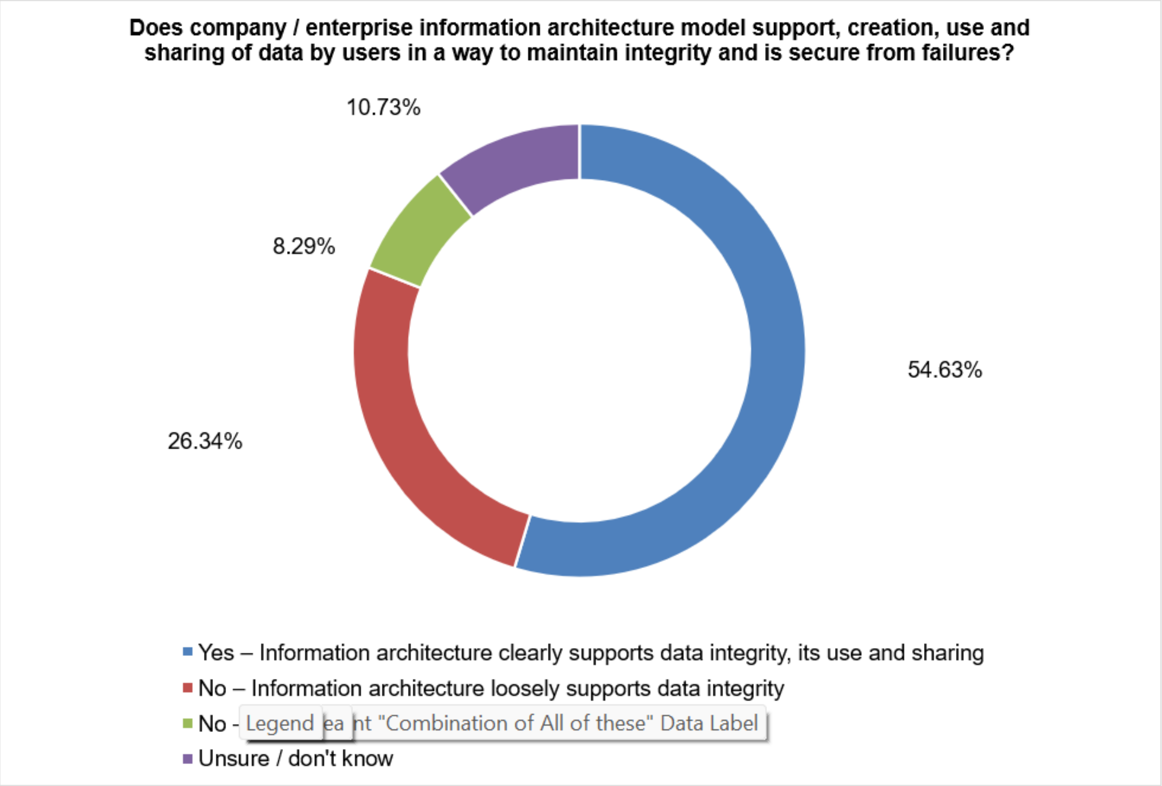


Figure 16

Table 22 shows that 54 of the total survey participants and Figure 17 shows that 26.34% of participants responded that 'Network' security is most important aspect of IT security.

Table 22: Area in IT security implementation

What is most important area in IT security implementation?		
Area	**No. of Responses**	**No. of Responses as % of Total**
Applications	31	15.12%
Server	21	10.24%
Storage	37	18.05%
Network	54	26.34%
Infrastructure	31	15.12%
Business Process	28	13.66%
Other	3	1.46%
Total	**205**	**100.00%**

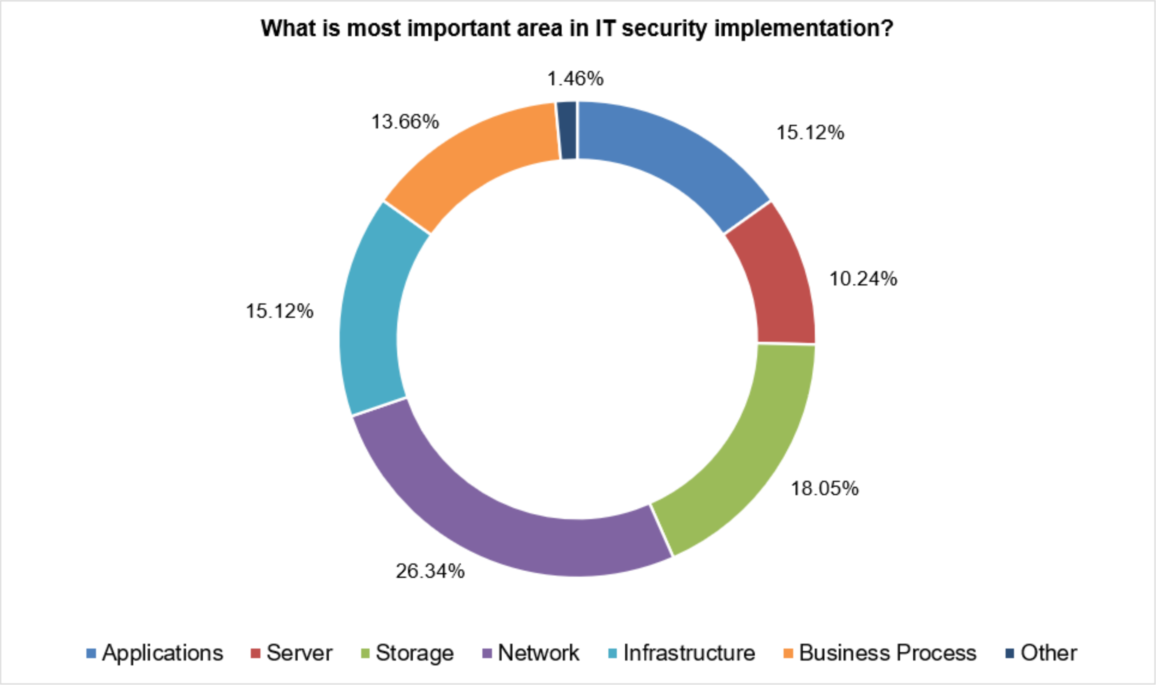


Figure 17

Table 23 shows that 136 of the total survey participants and Figure 18 shows that 66.34% of participants responded that ‘Data theft’ is most common security breach incident.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 23: Area in IT security implementation

What are most important areas of security breach incidents relating to data?		
Areas of security breach incidents	**No. of Responses**	**No. of Responses as % of Total**
Data Leakages	114	55.61%
Firewall Breach	117	57.07%
Data Theft	136	66.34%
Data Tampering	82	40.00%
Unauthorised data manipulation	80	39.02%
Unauthorised Data Deletion	58	28.29%

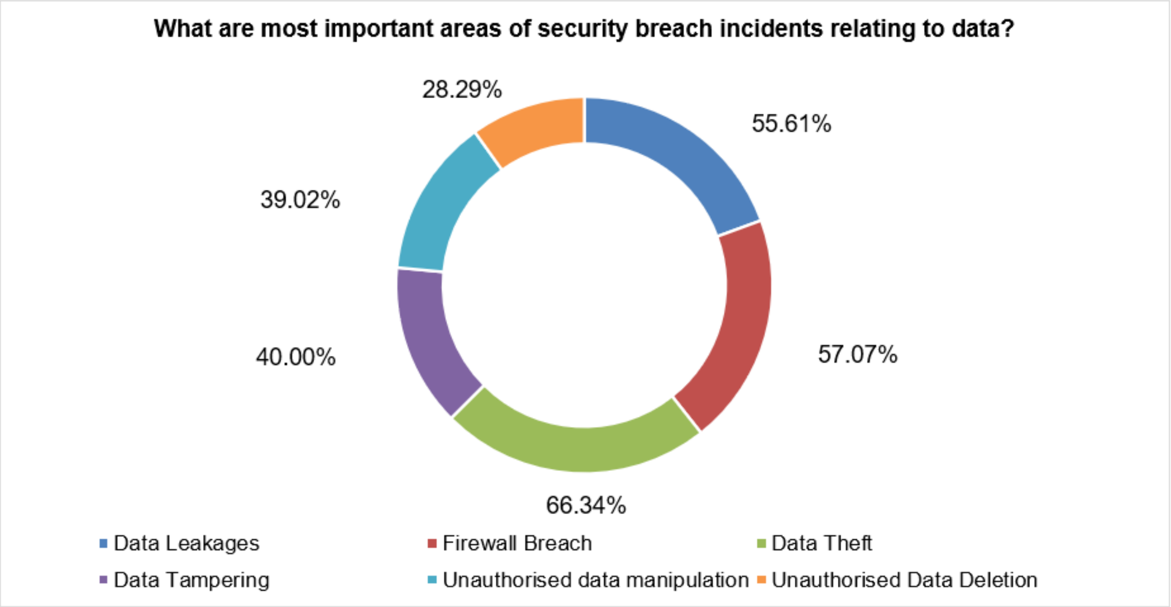


Figure 18

Table 24 shows that 155 of the total survey participants and Figure 19 shows that 75.61% of participants responded that ‘Firewall Rules’ are most common ‘security perimeter controls to monitor data leakage in the business.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 24: Security perimeter controls to monitor data leakages.

What is the security perimeter controls to monitor data leakages in the business?		
Security Perimeter Controls	**No. of Responses**	**No. of Responses as % of Total**
Data leakage Prevention Tools	97	47.32%
Firewall Rules	155	75.61%
Data Retention Tools	85	41.46%
Data Encryption Tools	96	46.83%

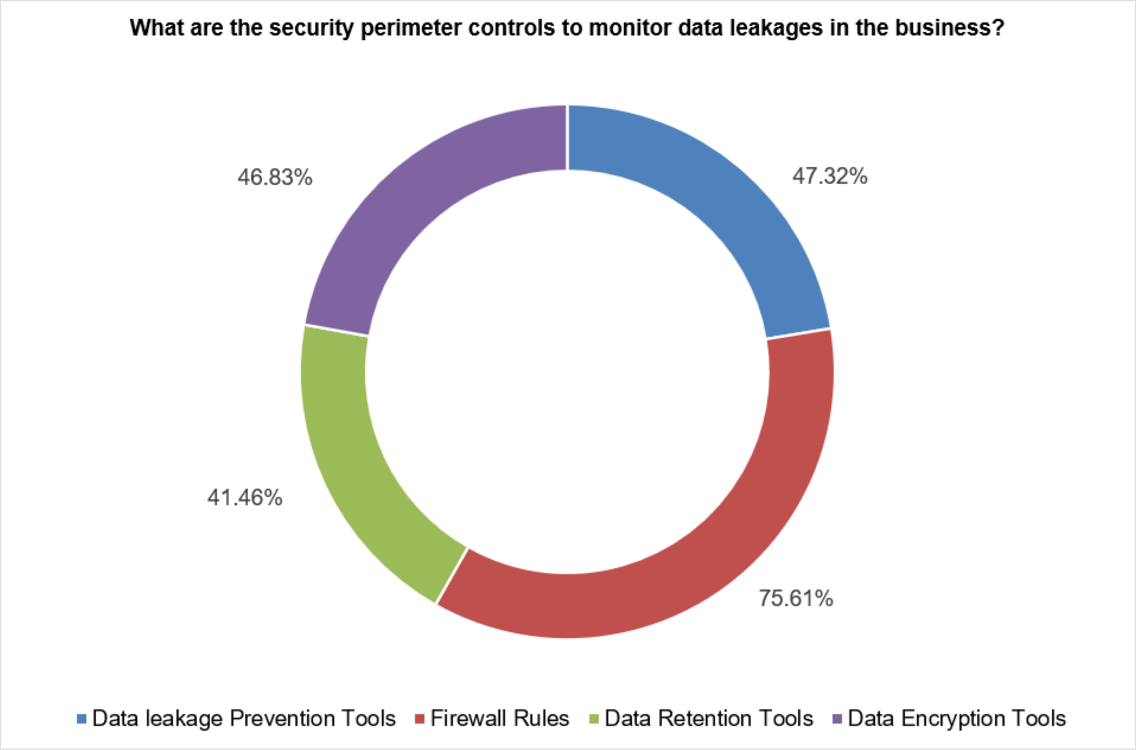


Figure 19

Table 25 shows that 76 of the total survey participants and Figure 20 shows that 37.07% of participants responded that ‘General Encryption is available for all types of data’ and is encryption methods.

Table 25: Data based encryption.

Does the business define the encryption methods based on data type?		
Security Perimeter Controls	**No. of Responses**	**No. of Responses as % of Total**
Yes	70	34.15%
No	28	13.66%
General Encryption is available for all types of data	76	37.07%
Unsure	31	15.12%
Total	**205**	**100.00%**

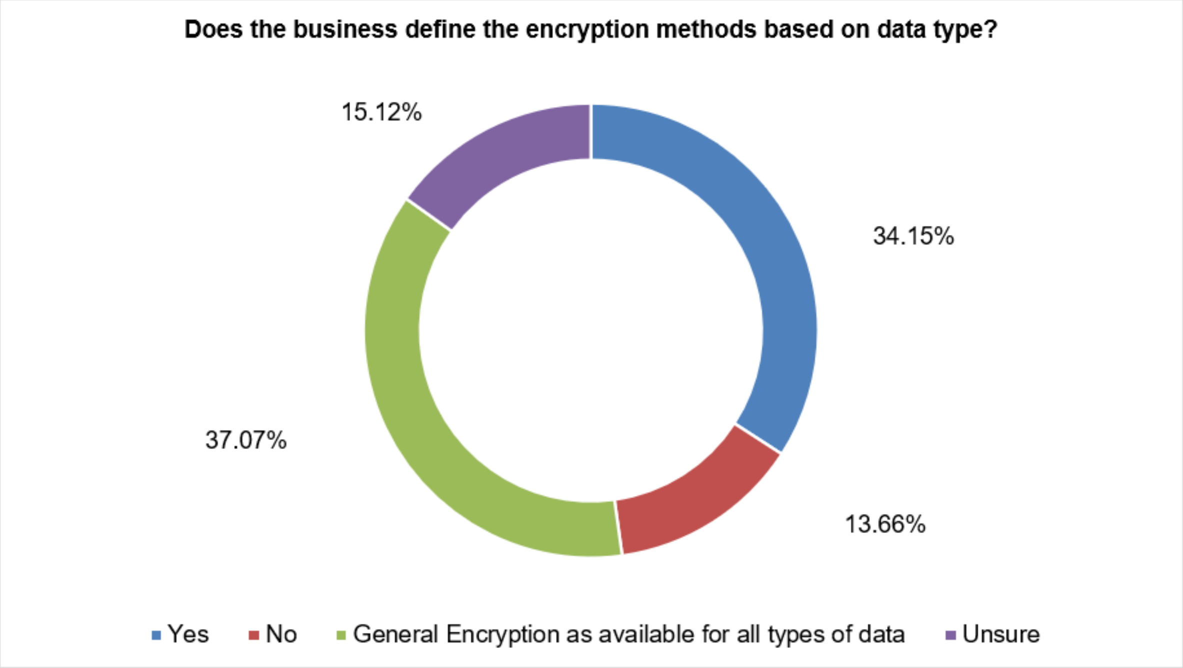


Figure 20

4.2.7 Reflection of research work concerning research question 1 (RQ1)

The responses from the survey for RQ1 shows the need of dedicated cloud governance team (mainly IT Operations (50.24%), IT Security (41.46%) and IT Risk management (33.17%)) and 3rd party cloud governance teams forming (19.51%) in survey. The survey results shows that dispersed cloud infrastructure management across organization making it work of team with varied skills sets. To deliver value for IT, cloud availability (42.44%), cloud accessibility (40.49%) and Application availability over cloud platform remain key areas. Cloud software component (60.00%) Cloud hardware components (46.83%), cloud security features (58.54%) and managing cloud operations (incidents, problems (43.41%) forms major part of cloud infrastructure management. High priority incident and security related incidents (56.59%) forms major concern for cloud infrastructure management. Availability of applications (37.07%) and cloud computing resources (storage (18.05%), network (26.34%)) forms major value delivery items of cloud infrastructure. Financial investment for cloud security and cloud management application continues to be need of cloud infrastructure. Data categorization well defined within an organization with personal data (63.41%) and customer data (62.93%) clearly identified by cloud users. Ongoing project plans (66.34%) continues to form key for cloud maturity model with change in IT architecture followed by IT support teams meeting with changing cloud infrastructure (53.66%) teams. Cloud operability for security perimeter controls to monitor data leakages in the business becomes more effective with cloud governance model using combination of data leakage prevention tools (47.32%), firewall rules (75.61%), data retention tools (41.46%) and data encryption Tools (46.83%). Cloud architecture maintains data integrity by recording security breach incident in the areas of data leakages, firewall breach, data theft, data tampering, unauthorised data manipulation and unauthorised data Deletion. Network security forms topmost priority for cloud security management. Data theft (66.34%), data leakages (55.61%) and firewall breach (57.07%) form major data loss areas. Firewall rules 75.61% forms key to manage security perimeter for cloud infrastructure. General data encryption methods (34.15%) are followed as a part of data encryption methods.

4.2.8 Prominent theme emerging for Research Question 1 (RQ1) from survey

The prominent theme emerging from responses received for RQ 1can be categorised in to following:

1. Participation of 3rd party cloud governance making cloud infrastructure management complex and demanding resources (financial, human, time)

2. Cloud security and cloud management application continue to demand investment

3. Cloud management continues to be challenging

4. There will be huge impact to the various data categories and application types used by Banking and Financial Services Corporations due to cloud architecture due to complexity in managing cloud infrastructure.

4.2.9 Discussion of research question 2 (RQ2)

Below table shows linking of RQ2 with 25 survey questions.

Table 26: Linking of RQ2 with 10 survey questions on cloud governance

Question No. in Questionnaire	Question Description	Research Question (RQ) No.	Research Area
1	What is the method to design Cloud governance framework?	RQ2	Cloud Governance
3	What are communication channels, methods, and frequency of cloud governance problems?	RQ2	Cloud Governance
10	How are cloud development and its objectives related with data security?	RQ2	Cloud Governance
11	How are cloud development and its objectives related with system security?	RQ2	Cloud Governance
13	How control over system changes to cloud architecture are controlled?	RQ2	Cloud Governance
16	How do you differentiate between governance needs of application, process, people, and infrastructure?	RQ2	Cloud Governance
17	How Cloud governance framework monitors and controls third party vendors and contractors?	RQ2	Cloud Governance
19	How are roles and responsibilities of various team aligning to Cloud value delivery?	RQ2	Cloud Governance
21	Do you evaluate existing governance framework and its effectiveness?	RQ2	Cloud Governance
22	How do you evaluate existing governance framework and its effectiveness?	RQ2	Cloud Governance

Table 27: Linking of RQ2 with 15 survey questions on cloud security

Question No. in Questionnaire	Question Description	Research Question (RQ) No.	Research Area
4	What are penetration testing cases to cover data security?	RQ2	Cloud Security
5	What are penetration testing cases to cover system security?	RQ2	Cloud Security
6	Are vulnerability assessment tools sufficient to report data security related incidents?	RQ2	Cloud Security
8	Is there any independent governance framework for data and system security?	RQ2	Cloud Security
9	What are bank specific security enforcement point to confirm data security?	RQ2	Cloud Security
10	Do you classify data based on data type?) Ex.: PII, Card Information, Transaction processing)	RQ2	Cloud Security
11	Does data categorization help to minimise risk of data loss?	RQ2	Cloud Security
12	Have you recently added / updated data security tools to meet existing threats and vulnerabilities?	RQ2	Cloud Security
16	Do you conduct regular training program with staff and 3rd Party vendors to bring awareness about data security?	RQ2	Cloud Security
17	How do you handle cyber-attack or DDoS?	RQ2	Cloud Security
18	Do you share findings of intrusion protection system (IPS) with other organizations / Banks?	RQ2	Cloud Security
21	Are traffic monitoring tools sufficient to filter packet level information?	RQ2	Cloud Security
33	Do you have data retention tools?	RQ2	Cloud Security
35	Is there a defined process to handle compromised devices?	RQ2	Cloud Security
42	Who is responsible for cloud user back-ground checks?	RQ2	Cloud Security

The column "Question No." in above table shows the sequence number in actual questionnaire emailed to participants.

Below shows the responses received for RQ2 from survey participants:

Table 28 shows that 92 of the total survey participants and Figure 21 shows that 44.88% of participants responded that 'Corporate / Enterprise Governance linked to IT Governance (management)' is method of the IT infrastructure governance (Cloud) framework at workplace.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 28: Method / design of the IT infrastructure governance (cloud) framework

What is the method / design of the IT infrastructure governance (Cloud) framework at your place of work?		
Method	**No. of Responses**	**No. of Responses as % of Total**
Corporate / Enterprise Governance linked to IT Governance (management)	92	44.88%
Independent IT infrastructure (Cloud) Governance Team within organization	43	20.98%
3rd party IT infrastructure (Cloud) Governance (Amazon (AWS), Microsoft Azure, Google Cloud (etc.))	70	34.15%

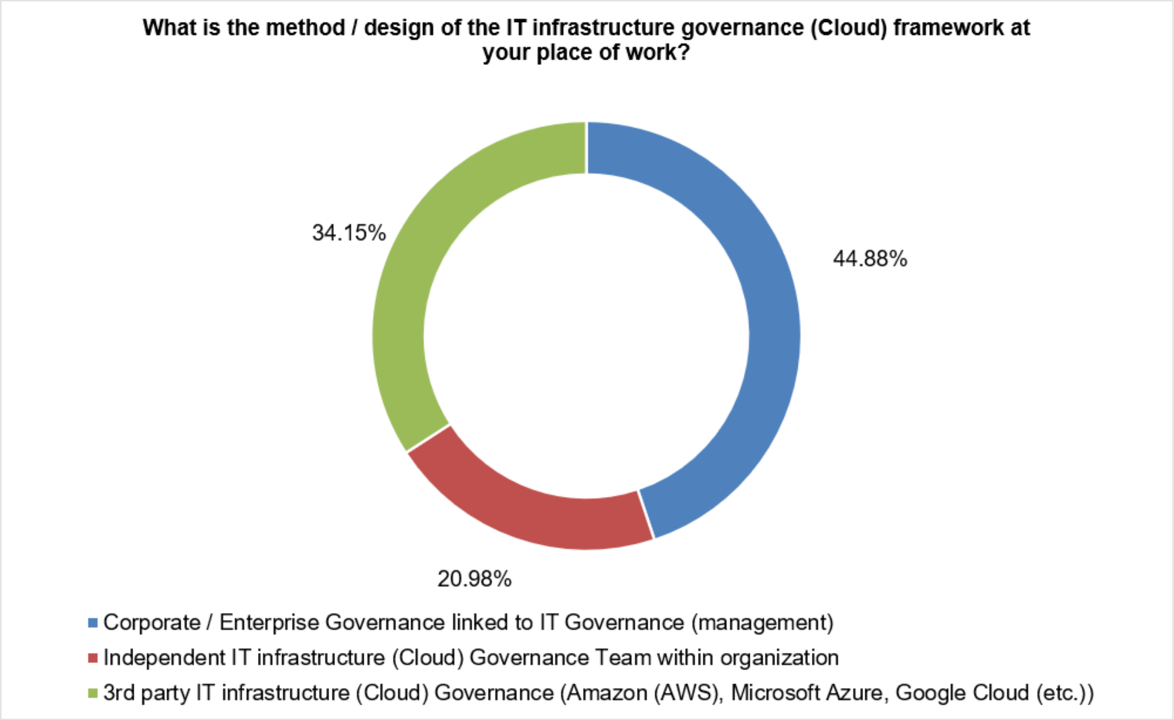


Figure 21

Table 29 shows that 115 of the total survey participants and Figure 22 shows that 56.10% of participants responded that ‘Email and Tele Conference and Incident and Problem Management’ represents the communication channels, methods, and frequency of addressing IT infrastructure (Cloud) governance problems.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 29: Communication channels within an organization

Which best represents the communication channels, methods, and frequency of addressing IT infrastructure (Cloud) governance problems?		
Communication Method	**No. of Responses**	**No. of Responses as % of Total**
Independent Meetings	76	37.07%
Email and Tele Conference	115	56.10%
Incident and Problem Management	115	56.10%
Need based engagement (Email, Calls, and Meeting etc.]	127	61.95%
Don't know / unsure	6	2.93%

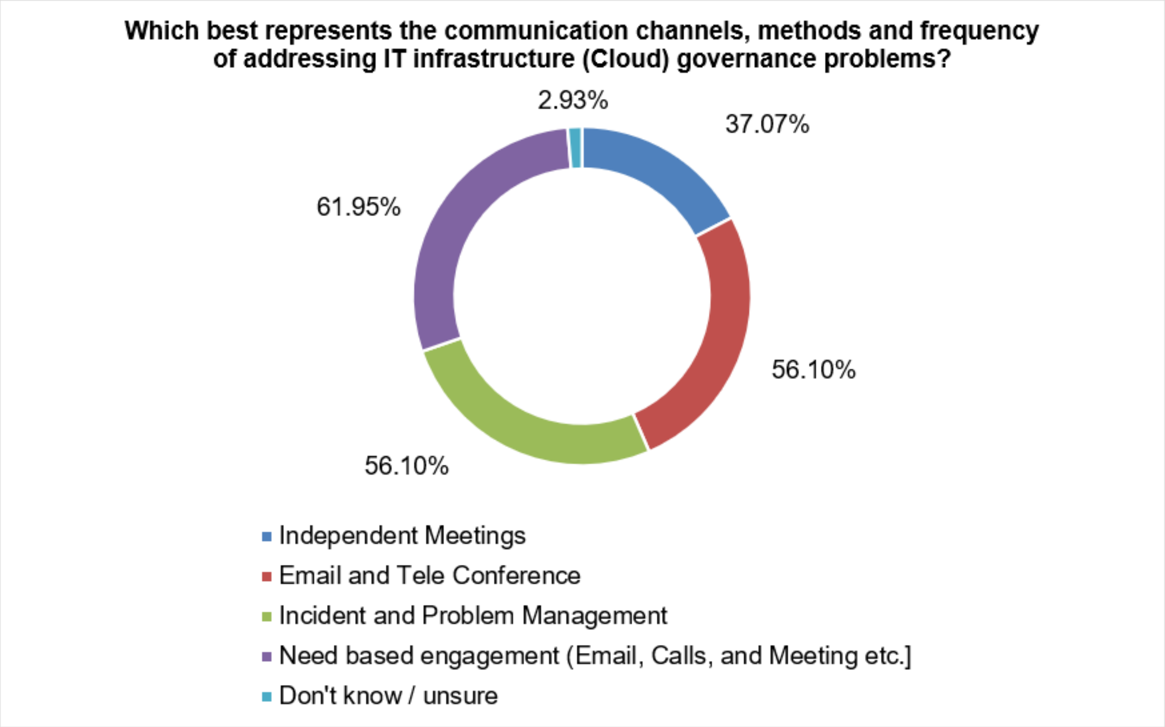


Figure 22

Table 30 shows that 98 of the total survey participants and Figure 23 shows that 47.80% of participants responded that primarily ‘On-Going Monitoring and Alert Mechanism’ are method to develop IT infrastructure (Cloud) and its objectives related to data security followed by ‘Combination of All of other options’ mentioned in survey question.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 30: Cloud security and IT infrastructure

How is the development of IT infrastructure (Cloud) and its objectives related to data security?		
Cloud Development	**No. of Responses**	**No. of Responses as % of Total**
Through Project Management	59	28.78%
On-Going Monitoring and Alert Mechanism	98	47.80%
Frequency Based Evaluation	50	24.39%
Combination of All of these	90	43.90%

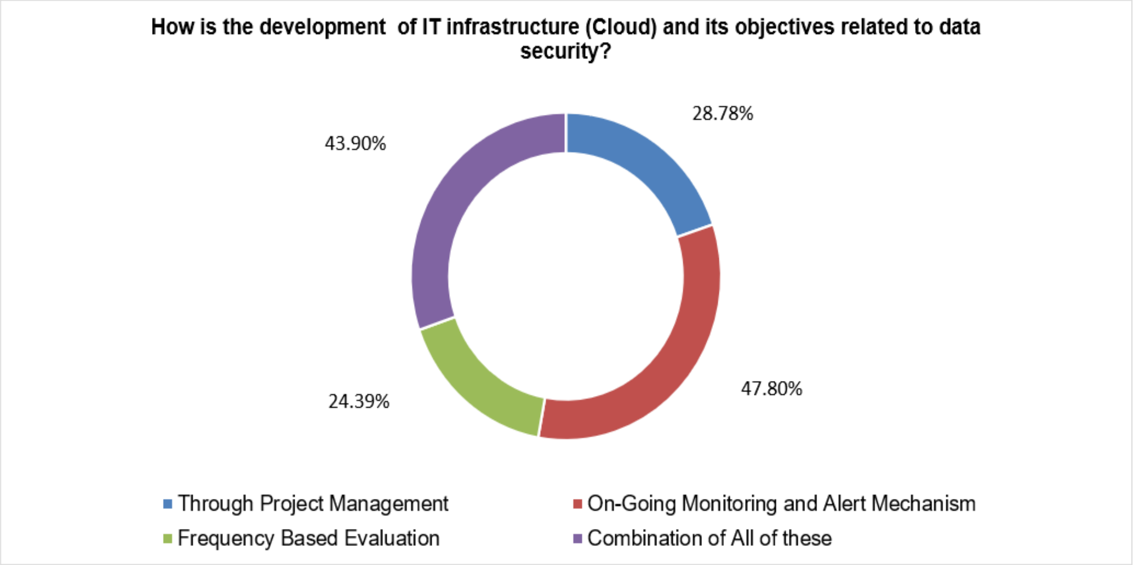


Figure 23

Table 31 shows that 101 of the total survey participants and Figure 24 shows that 49.27% of participants responded that ‘Collaborative efforts by all IT and Non-IT teams involved’ are method to control system changes to IT infrastructure (Cloud) architecture.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 31: System changes and control over IT infrastructure

How are the system changes to IT infrastructure (Cloud) architecture controlled?		
Control Methods	**No. of Responses**	**No. of Responses as % of Total**
Dedicated System Change and New code /fixes Release Management	74	36.10%
Collaborative efforts by all IT and Non-IT teams involved	101	49.27%
Partially controlled by IT management (Governance) Team	63	30.73%
No formal Structure, issues are handled on need basis	51	24.88%

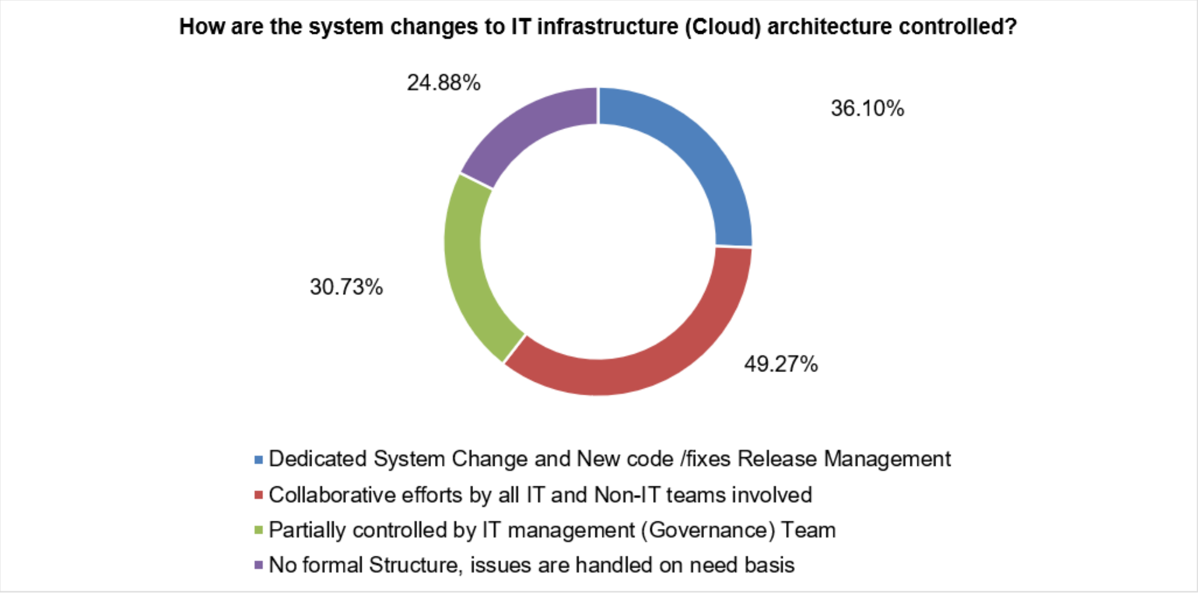


Figure 24

Table 32 shows that 74 of the total survey participants and Figure 25 shows that 36.10% of participants responded that ‘Enterprise Management / Governance team is accountable for overall IT infrastructure (Cloud) infrastructure’ is the method to differentiate between management / Governance needs of application, process, people, and infrastructure.

Table 32: Differentiate between management / governance needs of application, process, people, and infrastructure.

How do you differentiate between management / Governance needs of application, process, people, and infrastructure?		
Differentiate	**No. of Responses**	**No. of Responses as % of Total**
Each Area has dedicated resource who is accountable	49	23.90%
Enterprise Management / Governance team is accountable for overall IT infrastructure (Cloud) infrastructure	74	36.10%
Joint Responsibility between leaders of various team	73	35.61%
Others	9	4.39%
Total	**205**	**100.00%**

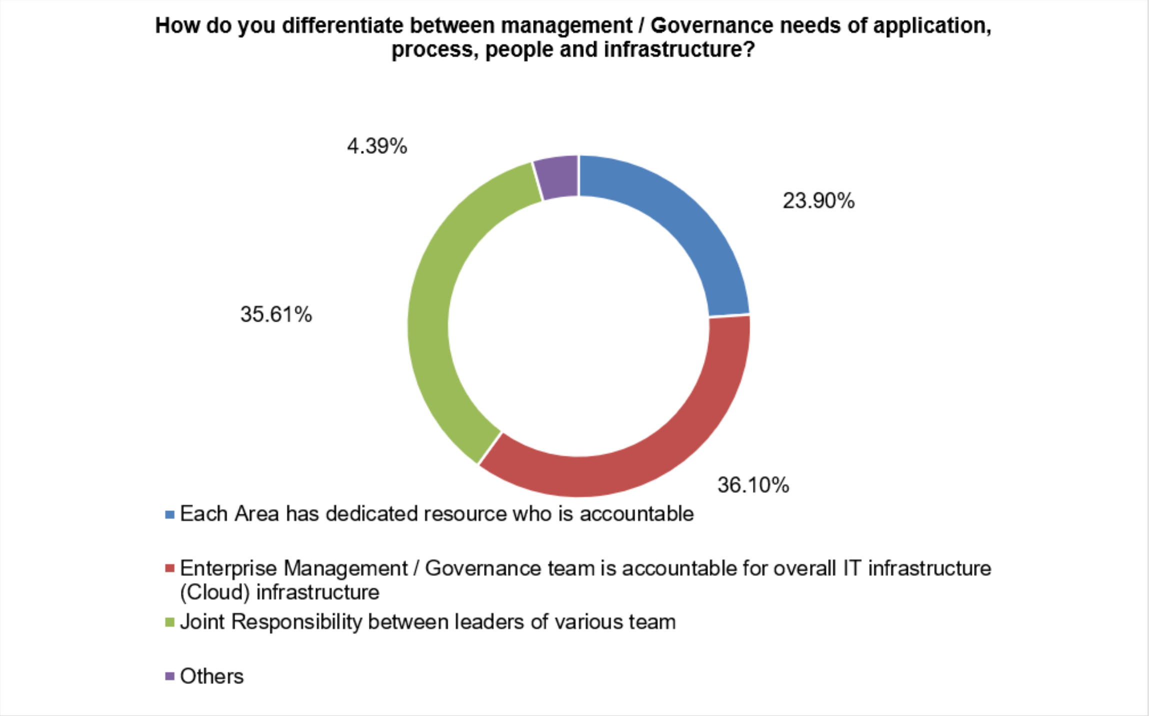


Figure 25

Table 33 shows that 83 of the total survey participants and Figure 26 shows that 40.49% of participants responded that 'Contractual Agreements / Legal IT Contracts and Guidelines issue based on business needs' is the method to monitor and control 3rd party vendors and contractors.

Table 33: Monitoring and control methods IT infrastructure

How does the businesses IT infrastructure (Cloud) governance / management framework monitor and control 3rd party vendors and contractors?		
Monitoring and Control Methods	**No. of Responses**	**No. of Responses as % of Total**
Contractual Agreements / Legal IT Contracts	18	8.78%
Guidelines issue based on business needs	47	22.93%
Both A & B	83	40.49%
Regular Audit	19	9.27%
C & D	38	18.54%
Total	**205**	**100.00%**

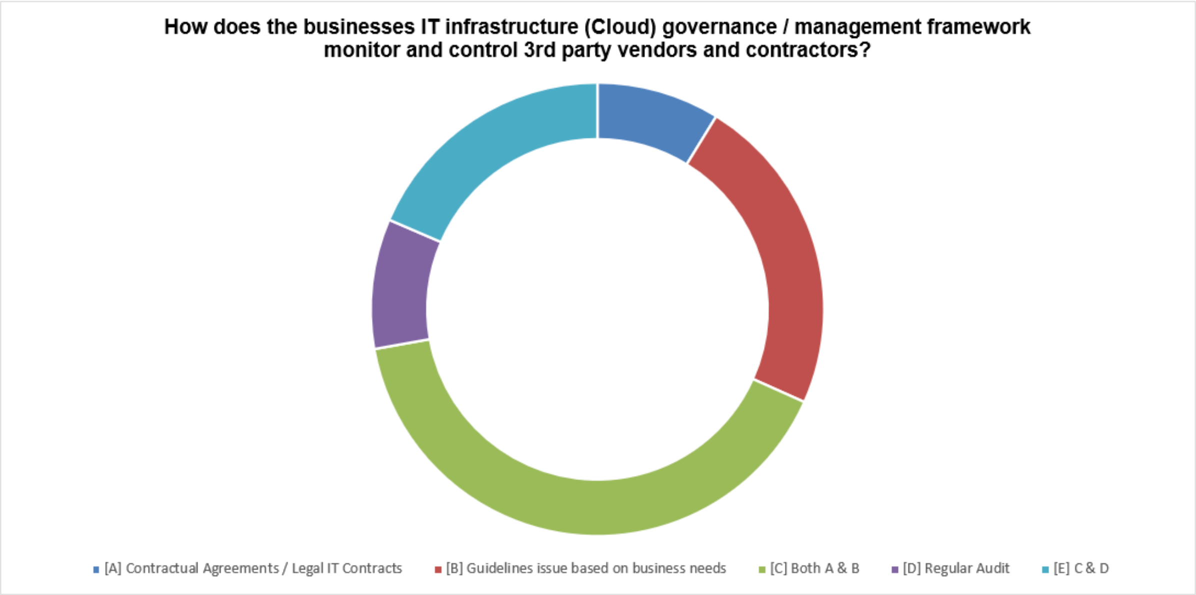


Figure 26

Table 34 shows that 138 of the total survey participants and Figure 27 shows that 67.32% of participants responded that 'Through Roles and Responsibility Description' is the method for various IT teams to align IT infrastructure (Cloud) value delivery.

Table 34: Value delivery of IT infrastructure

How do roles and responsibilities of various IT teams align to IT infrastructure (Cloud) value delivery?		
Monitoring and Control Methods	**No. of Responses**	**No. of Responses as % of Total**
Through Roles and Responsibility Description	138	67.32%
Through Project Delivery Needs	109	53.17%
Others (specify)	4	1.95%
Total	**205**	**100.00%**

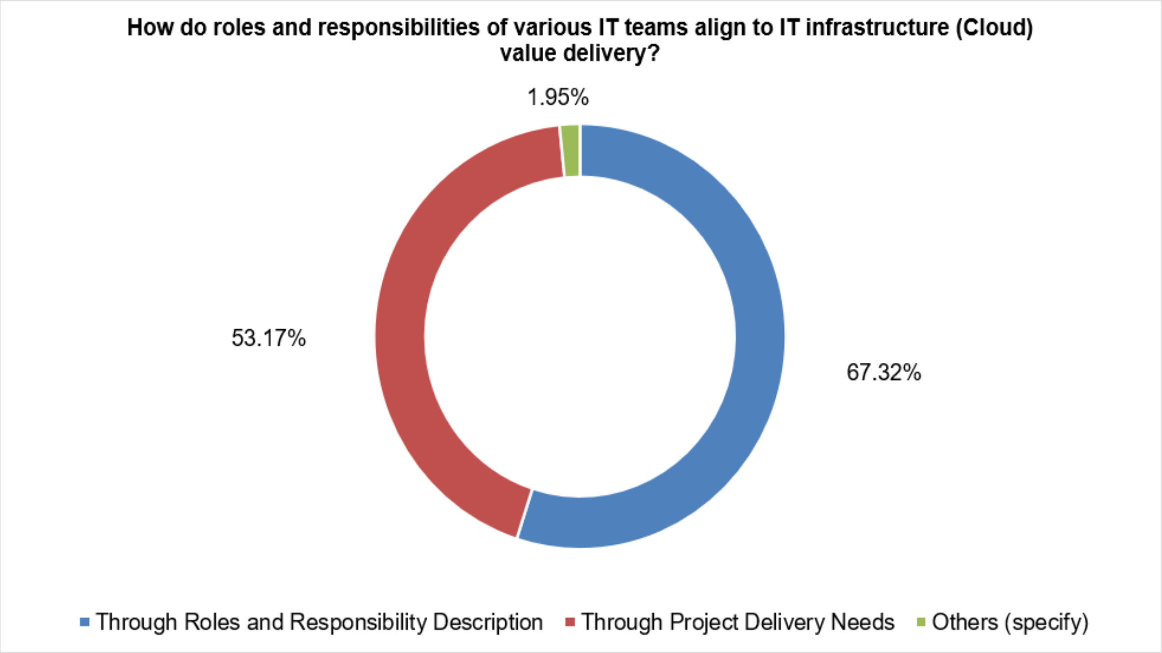


Figure 27

Table 35 shows that 104 of the total survey participants and Figure 28 shows that 50.73% of participants responded that 'On a need-based upgrade to policies and procedure' is the method for the business to evaluate existing IT infrastructure (Cloud) management / governance framework and its effectiveness.

Table 35: IT infrastructure and its effectiveness 1

Does the business evaluate existing IT infrastructure (Cloud) management / governance framework and its effectiveness? If so, how often?		
Evaluation Duration	**No. of Responses**	**No. of Responses as % of Total**
Yes - Constant upgrades to policies and procedures	76	37.07%
Yes - On a need-based upgrade to policies and procedure	104	50.73%
No upgrade unless annual goals are achieved	25	12.20%
Total	**205**	**100.00%**

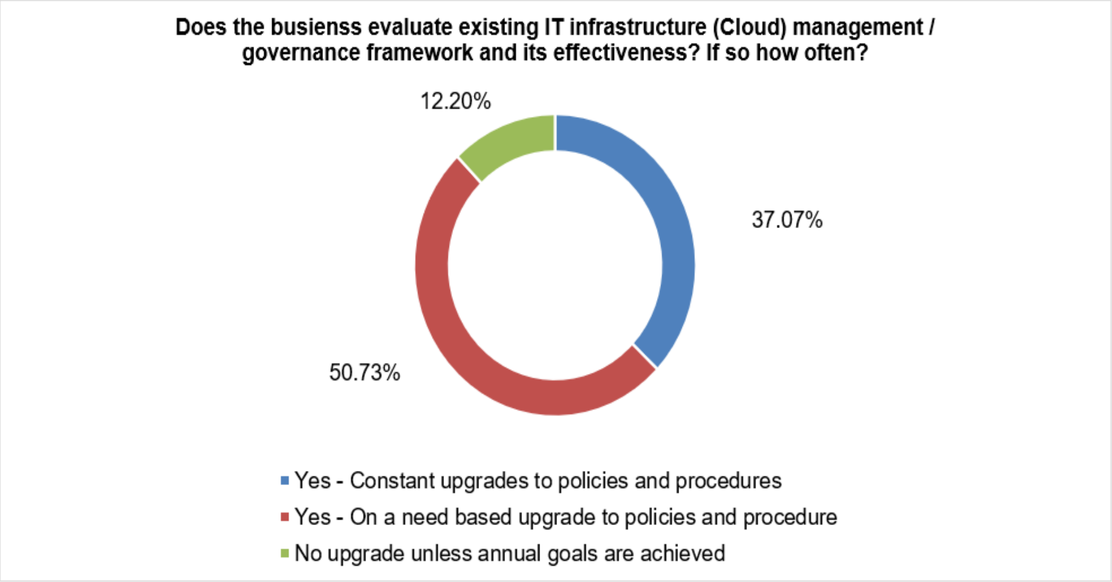


Figure 28

Table 36 shows that 93 of the total survey participants and Figure 29 shows that 45.37% of participants responded that ‘Evaluate IT management / governance goals with enterprise / company goals’ is the method for the business to evaluate existing IT infrastructure (Cloud) management / governance framework and its effectiveness.

Table 36: IT infrastructure and its effectiveness 2

How does the business evaluate existing IT infrastructure (Cloud) management / governance framework and its effectiveness?		
Evaluation Method	**No. of Responses**	**No. of Responses as % of Total**
Evaluate IT management / governance goals with enterprise / company goals	93	45.37%
Need based evaluation if failures observed in reaching IT Goals	89	43.41%
No evaluation unless annual enterprise goals are not achieved	23	11.22%
Total	**205**	**100.00%**

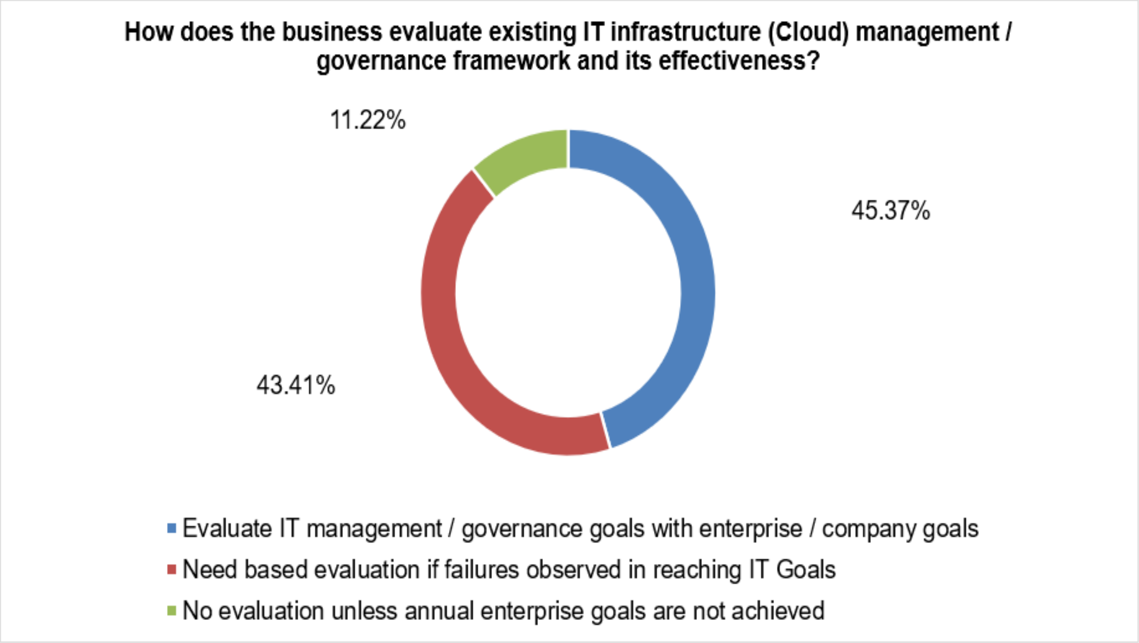


Figure 29

Table 37 shows that 123 of the total survey participants and Figure 30 shows that 60.00% of participants responded that 'Server Level Control' is the method for penetration testing cases to cover data security.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 37: Penetration testing for data security

Which penetration testing cases are to cover data security?		
Penetration Testing Method	**No. of Responses**	**No. of Responses as % of Total**
Application-Level Control	108	52.68%
Server Level Control	123	60.00%
Network Level Control	106	51.71%
Firewall Rules	104	50.73%

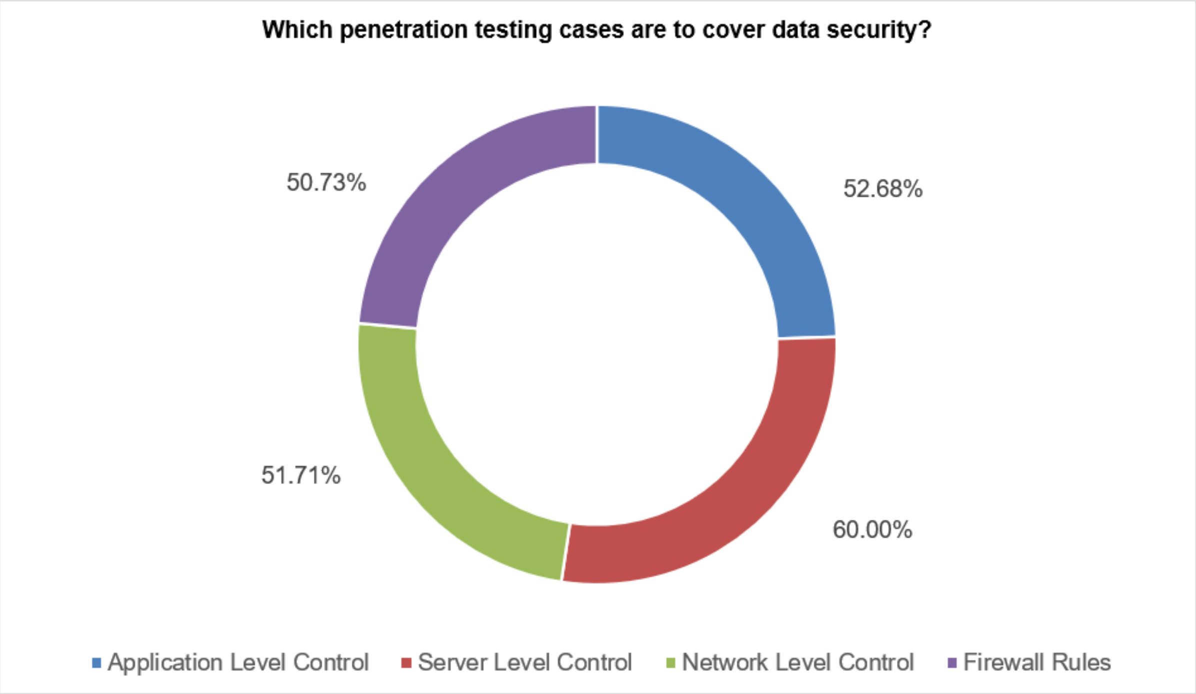


Figure 30

Table 38 shows that 122 of the total survey participants and Figure 31 shows that 59.51% of participants responded that ‘Server Level Control’ is the method for penetration testing cases to cover system security.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 38: Penetration testing for system security

What types of penetration (deep intrusion) testing cases used to cover system security?		
Penetration Testing Method	**No. of Responses**	**No. of Responses as % of Total**
Application-Level Control	99	48.29%
Server Level Control	122	59.51%
Network Level Control	108	52.68%
Firewall Rules	108	52.68%

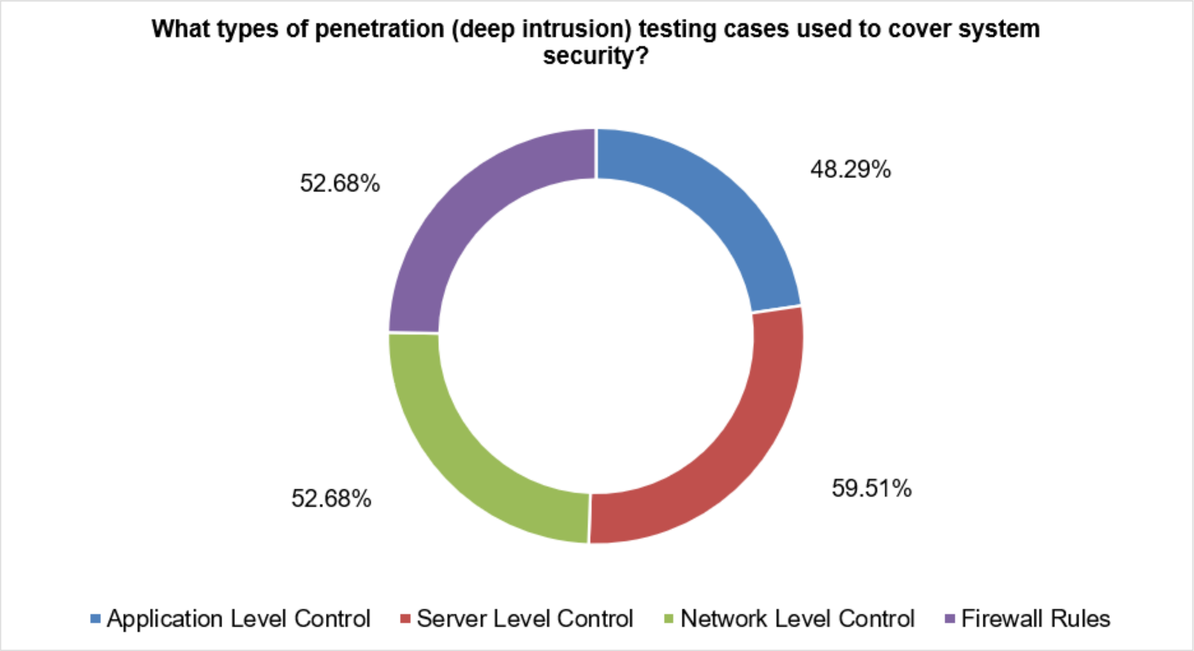


Figure 31

Table 39 shows that 123 of the total survey participants and Figure 32 shows that 40.49% of participants responded that vulnerability assessment tools are sufficient to report data security related incidents.

Table 39: Vulnerability assessment tools for data security

Are vulnerability assessment tools sufficient to report data security related incidents?		
Assessment Tool Usage	**No. of Responses**	**No. of Responses as % of Total**
Yes	83	40.49%
No	60	29.27%
Unsure / don't know	62	30.24%
Total	**205**	**100.00%**

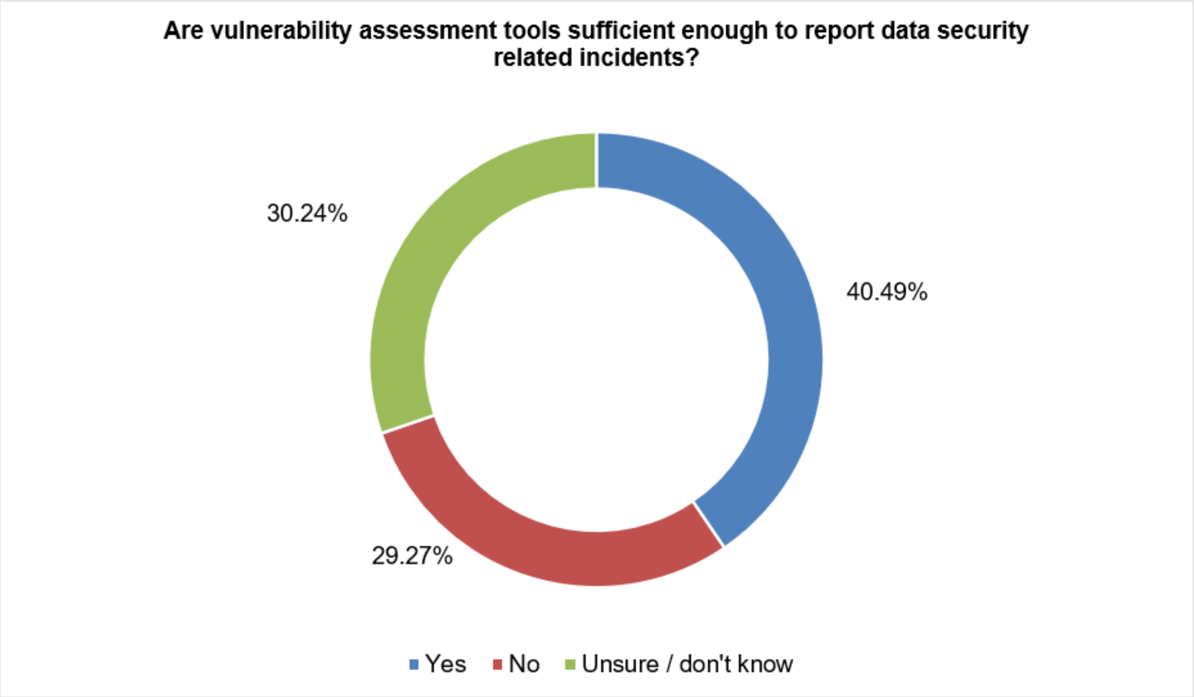


Figure 32

Table 40 shows that 106 of the total survey participants and Figure 33 shows that 51.71% of participants responded that there is an independent management / governance framework for data and system security in the business.

Table 40: Independent management / governance framework for data and system security

Is there an independent management / governance framework for data and system security in the business?		
Assessment Tool Usage	**No. of Responses**	**No. of Responses as % of Total**
Yes	106	51.71%
No	71	34.63%
Unsure / don't know	28	13.66%
Total	**205**	**100.00%**

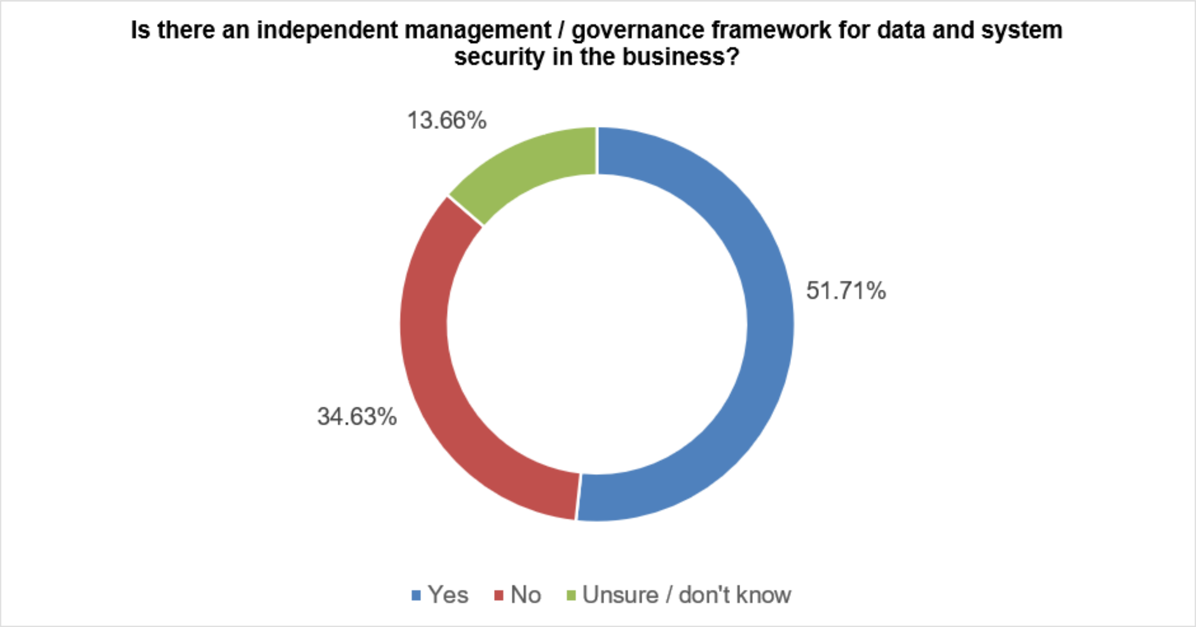


Figure 33

Table 41 shows that 90 of the total survey participants and Figure 34 shows that 43.90% of participants responded that ‘Education to Staff and 3rd Party Vendor about importance of data’ is the method to Bank specific security enforcement points used to confirm data security.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 41: Bank specific security enforcement points

What are Bank specific security enforcement points used to confirm data security?		
Bank specific security enforcement points	**No. of Responses**	**No. of Responses as % of Total**
Dedicated data / content analysis tool for Bank / company	65	31.71%
Education to Staff and 3rd Party Vendor about importance of data	90	43.90%
Secure data transfer protocols	77	37.56%
Role Based access to Data over shared drives	50	24.39%
All of these	56	27.32%

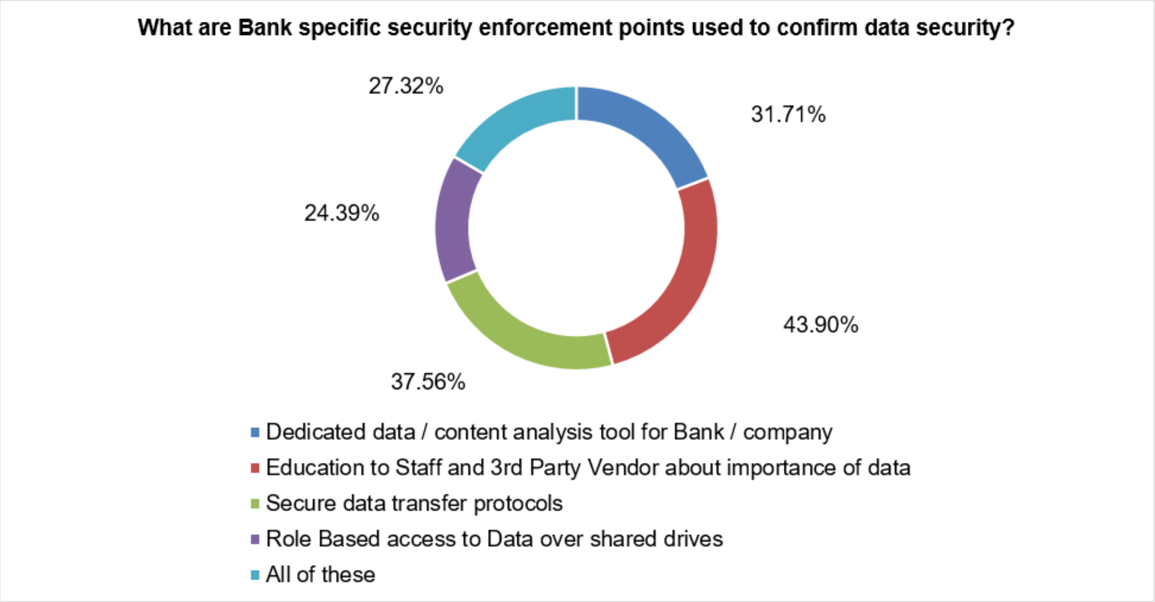


Figure 34

Table 42 shows that 146 of the total survey participants and Figure 35 shows that 71.22% of participants responded that 'business classify data based on data type'.

Table 42: Data type categorization

Does the business classify data based on data type? (e.g. Personal Information, Credit Card Information, Financial Transaction processing)		
Data Type Categorization	**No. of Responses**	**No. of Responses as % of Total**
Yes	146	71.22%
No	44	21.46%
Unsure	15	7.32%
Total	**205**	**100.00%**

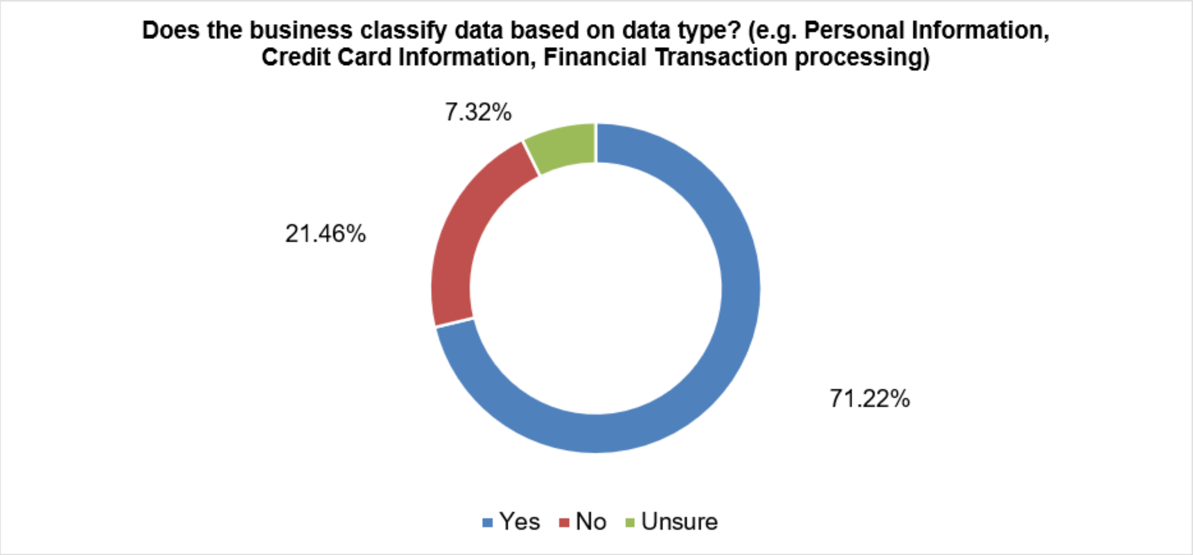


Figure 35

Table 43 shows that 131 of the total survey participants and Figure 36 shows that 63.90% of participants responded that data categorization help to minimise risk of data loss in the business.

Table 43: Risk minimization and data category

Does data categorization help to minimise risk of data loss in the business?		
Risk Minimization	**No. of Responses**	**No. of Responses as % of Total**
Yes	131	63.90%
No	49	23.90%
Unsure	25	12.20%
Total	**205**	**100.00%**

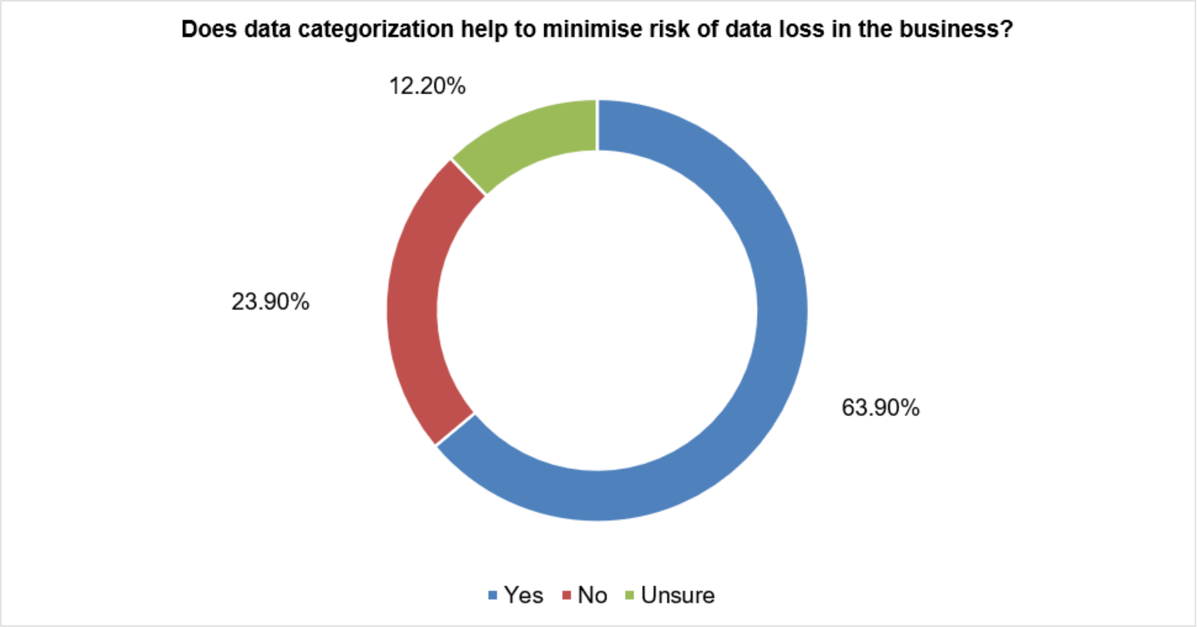


Figure 36

Table 44 shows that 126 of the total survey participants and Figure 37 shows that 61.46% of participants responded that business recently added / updated data security tools to meet existing threats and vulnerabilities.

Table 44: New security tools to mitigate risks.

Has the business recently added / updated data security tools to meet existing threats and vulnerabilities?		
Security Tool Implementation	**No. of Responses**	**No. of Responses as % of Total**
Yes	126	61.46%
No	57	27.80%
Unsure	22	10.73%
Total	**205**	**100.00%**

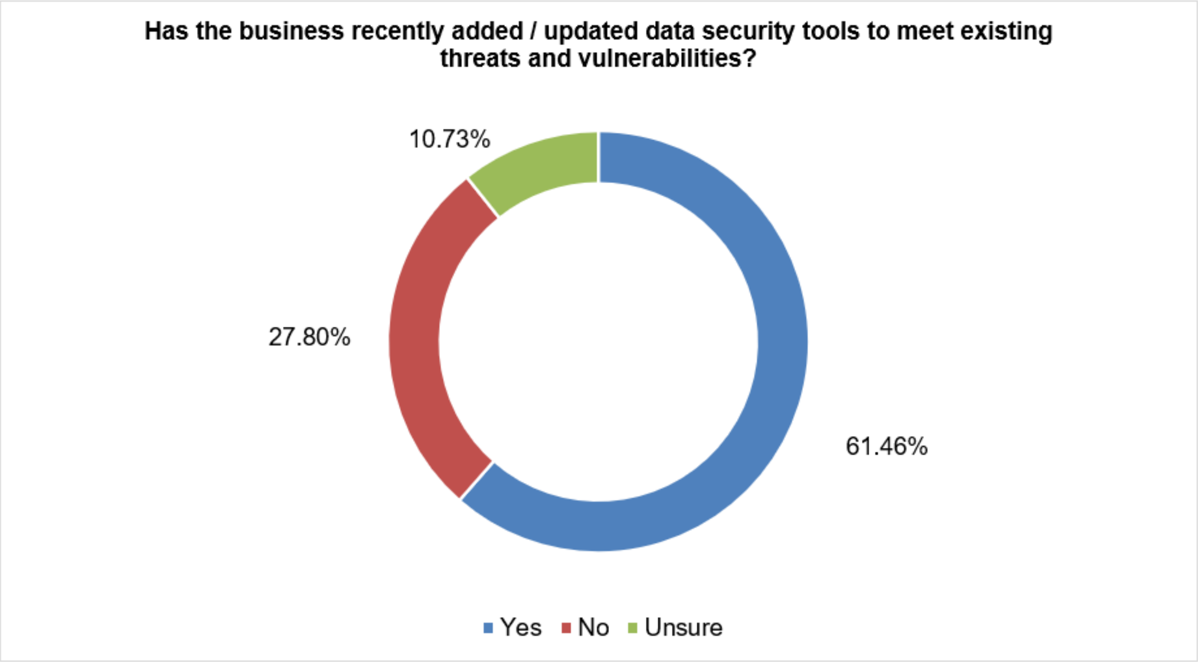


Figure 37

Table 45 shows that 124 of the total survey participants and Figure 38 shows that 60.49% of participants responded that business conduct regular training program with staff and 3rd Party vendors to bring awareness about data security.

Table 45: Training program for data security

Does the business conduct regular training program with staff and 3rd Party vendors to bring awareness about data security?		
Security Tool Implementation	**No. of Responses**	**No. of Responses as % of Total**
Yes	124	60.49%
No	65	31.71%
Unsure	16	7.80%
Total	**205**	**100.00%**

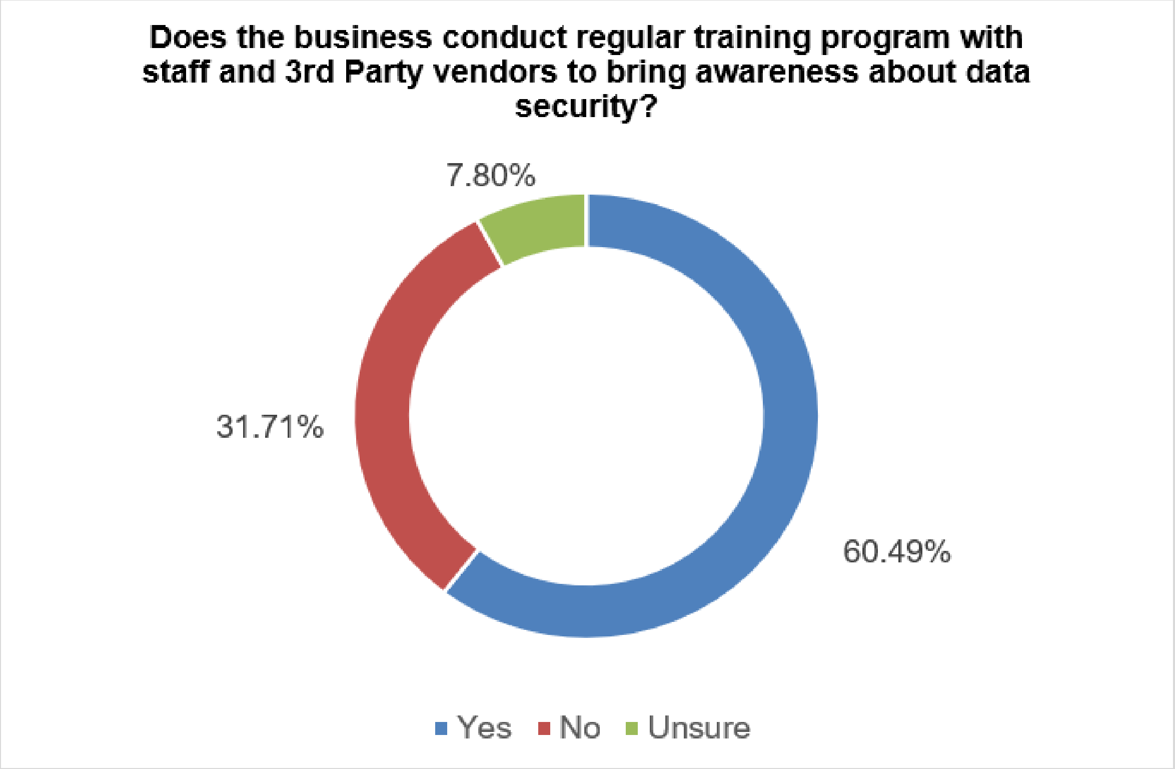


Figure 38

Table 46 shows that 84 of the total survey participants and Figure 39 shows that 40.98% of participants responded that ‘Through Quarantine and Block features with existing tools’ and ‘Updating Firewall Rules’ is the method to business handle cyber-attacks or Distributed Denial of Services (DDoS).

Table 46: Cyber-attacks/DDoS mitigation and IT infrastructure

How does the business handle cyber-attacks or Distributed Denial of Services (DDoS)?		
Cyber Attacks/DDoS Mitigation	**No. of Responses**	**No. of Responses as % of Total**
Through Quarantine and Block features with existing tools	84	40.98%
Through Honey Pot Tools to monitor behaviour of attack and develop attack vector specific	41	20.00%
Updating Firewall Rules	84	40.98%
All of these	63	30.73%
Total	**205**	**100.00%**

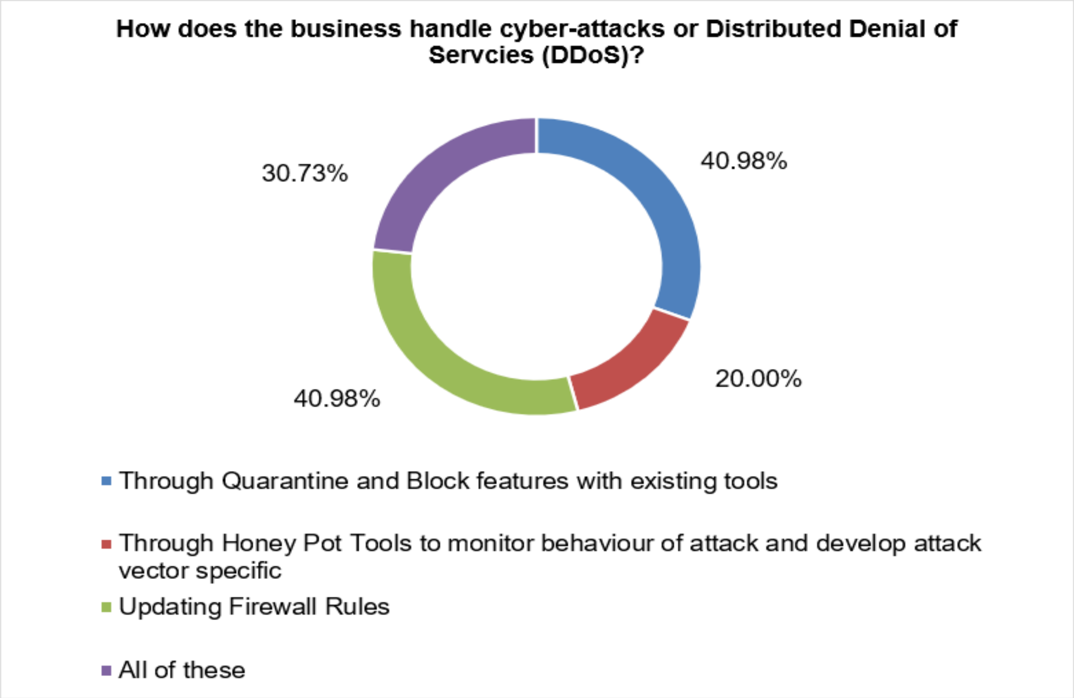


Figure 39

Table 47 shows that 132 of the total survey participants and Figure 40 shows that 64.39% of participants responded that they do not share findings of intrusion protection system (IPS) with other organizations.

Table 47: Information sharing on Cyberattacks.

Do you share findings of intrusion protection system (IPS) with other organizations?		
Cyber Attacks/DDoS Mitigation	**No. of Responses**	**No. of Responses as % of Total**
Yes	73	35.61%
No	132	64.39%
Total	**205**	**100.00%**

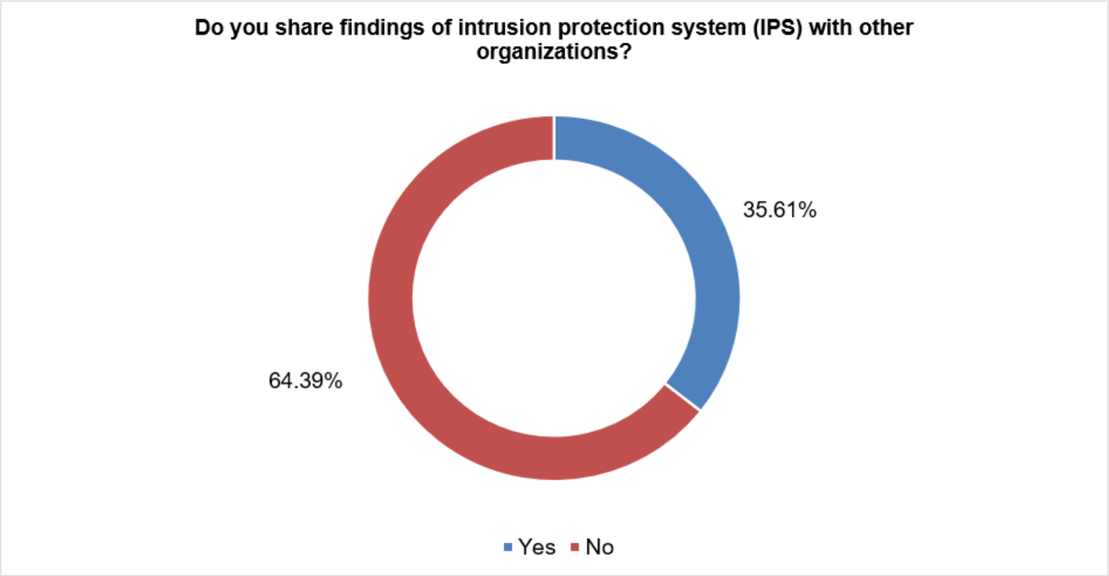


Figure 40

Table 48 shows that 71 of the total survey participants and Figure 41 shows that 34.63% of participants responded that traffic monitoring tools sufficient to filter packet level information for the business.

Table 48: User traffic monitoring tools and information filtering

Are traffic monitoring tools sufficient to filter packet level information for the business?		
Traffic Monitoring Tools	**No. of Responses**	**No. of Responses as % of Total**
Yes	71	34.63%
No	23	11.22%
Only to monitor traffic Load	42	20.49%
Separate Tool for content monitoring	25	12.20%
Unsure	44	21.46%
Total	**205**	**100.00%**

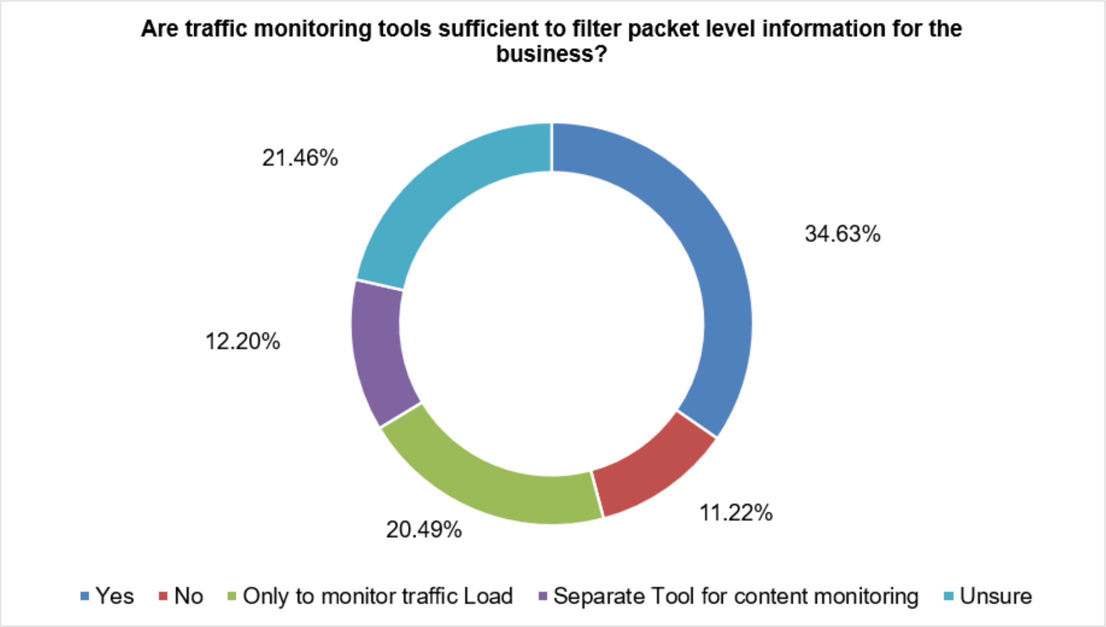


Figure 41

Table 49 shows that 91 of the total survey participants and Figure 42 shows that 44.39% of participants responded that business have and use data retention tools for data loss and data deletion.

Table 49: Data retention tools and data loss prevention

Does the business have and use data retention tools?		
Data Retention Tools	**No. of Responses**	**No. of Responses as % of Total**
Yes – for all types of data loss and data deletion	91	44.39%
Yes – only for accidental data deletion on available devices	49	23.90%
No – there is no data retention tools available	31	15.12%
Data retention for last back up via share drive is possible	34	16.59%
Total	**205**	**100.00%**

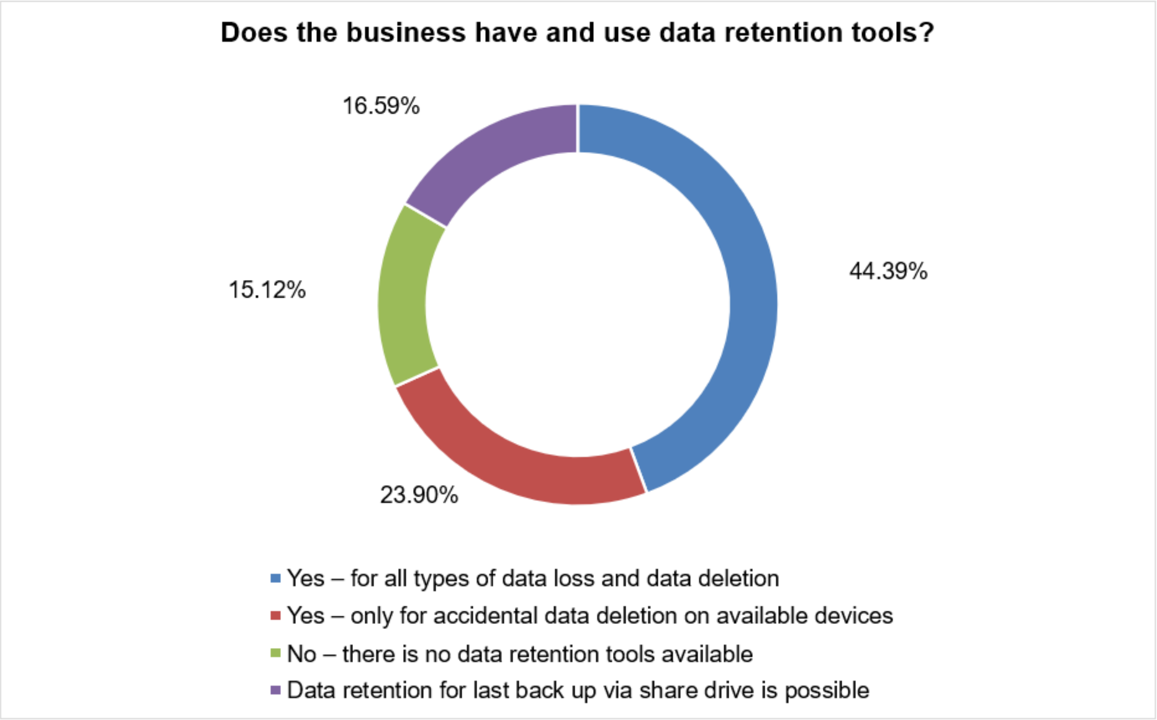


Figure 42

Table 50 shows that 90 of the total survey participants and Figure 43 shows that 43.90% of participants responded that ‘Lost devices are isolated and monitored for further investigation’ for data deletion.

Table 50: Process to handle lost devices.

What methods are used for data deletion for lost devices?		
Data Retention Tools	**No. of Responses**	**No. of Responses as % of Total**
Lost devices are de-activated permanently from network connectivity	87	42.44%
Lost devices are isolated and monitored for further investigation	90	43.90%
Devices other than laptop devices are not allowed to be used over IT Infrastructure (Cloud)	47	22.93%
No process to remove data from lost devices	37	18.05%
Total	**205**	**100.00%**

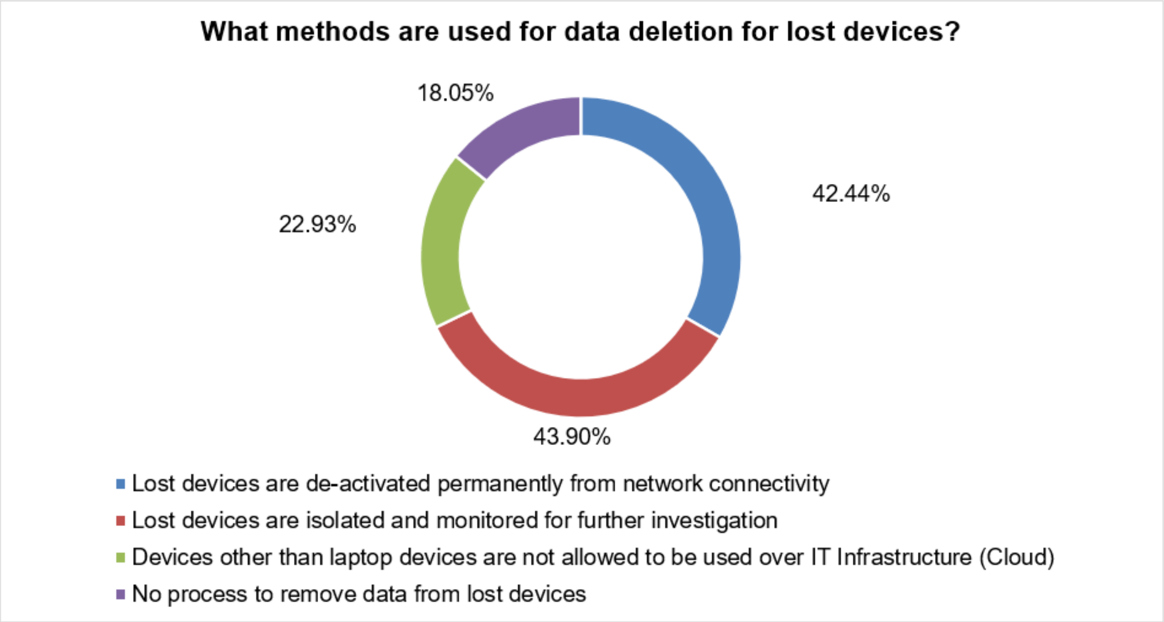


Figure 43

Table 51 shows that 96 of the total survey participants and Figure 44 shows that 46.83% of participants responded that ‘Compromised devices can be identified and isolated from cloud network’ in the event if devices are compromised.

Table 51: Process to handle compromised devices.

Is there a defined process to handle compromised devices?		
Data Retention Tools	**No. of Responses**	**No. of Responses as % of Total**
Yes – Compromised devices can be identified and isolated from cloud network	96	46.83%
Yes – Compromised devices are identified to certain extent based on damage	59	28.78%
No – There is no technique to identify compromised devices	50	24.39%
Total	**205**	**100.00%**

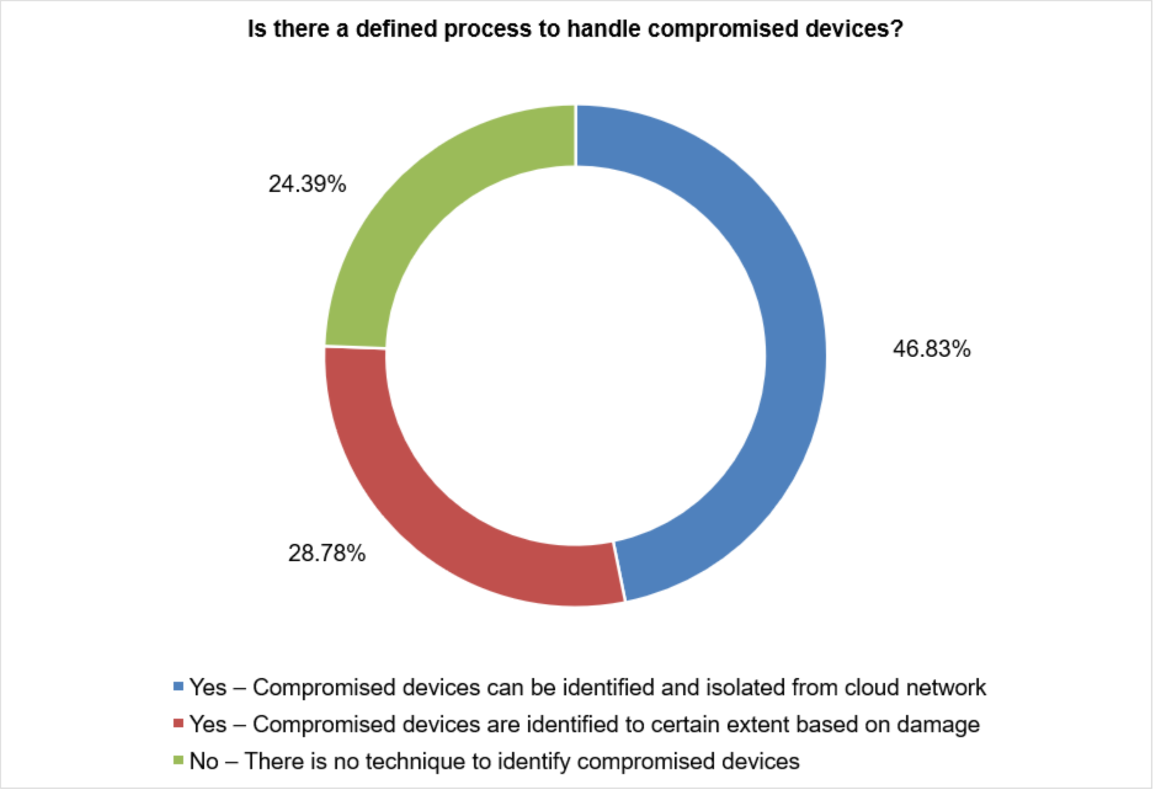


Figure 44

Table 52 shows that 76 of the total survey participants and Figure 45 shows that 37.07% of participants responded that 'IT Security through 3rd Party Services' are responsible for IT Infrastructure (Cloud) user back-ground checks.

Table 52: Backgrounds checks for IT infrastructure users

Who is responsible for IT Infrastructure (Cloud) user back-ground checks?		
User Back-ground check	**No. of Responses**	**No. of Responses as % of Total**
Human Resources through 3rd Party services	47	22.93%
IT Security through 3rd Party Services	76	37.07%
No Back-ground check conducted	33	16.10%
Back-ground checks only for 3rd Party vendors through 3rd party Services by Human resources	28	13.66%
Unsure	21	10.24%
Total	**205**	**100.00%**

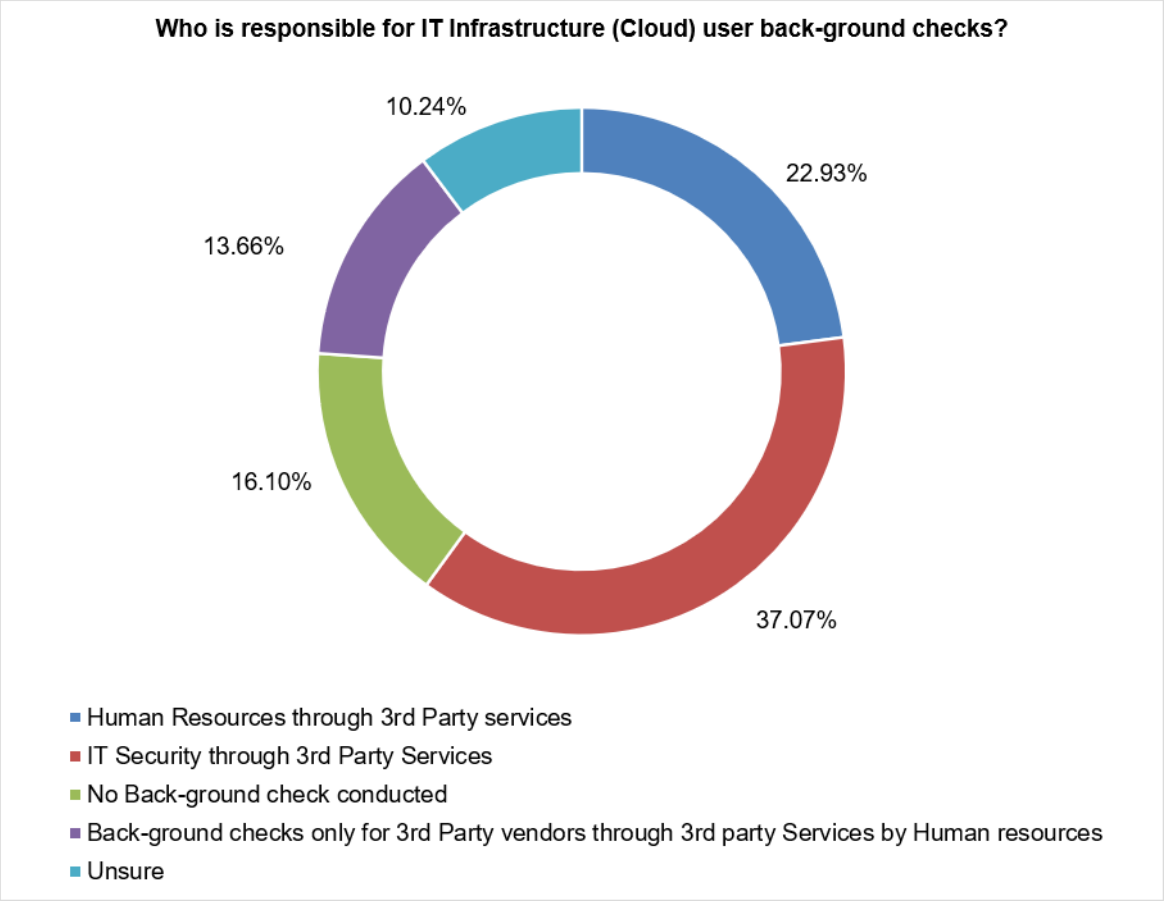

Who is responsible for IT Infrastructure (Cloud) user back-ground checks?
10.24%
22.93%
13.66%
16.10%
37.07%
Human Resources through 3rd Party services
IT Security through 3rd Party Services
No Back-ground check conducted
Back-ground checks only for 3rd Party vendors through 3rd party Services by Human resources
Unsure

Figure 45

Table 53: RQ1 and RQ2 in survey questions on cloud governance

Question No.	Question Description	Research Question (RQ) No.	Research Area
23	Do you have clear strategic plan to assess data security and system security at governance forum?	RQ1, RQ2	Cloud Governance
24	Does project portfolio management office (PPMO) clearly define, evaluates, prioritise, selects, initiates, manages, and controls data and system security related changes as a part of project delivery?	RQ1, RQ2	Cloud Governance
26	How do you manage integrity of data stored in electronic form such as databases, data warehouse and data archives?	RQ1, RQ2	Cloud Governance
27	Does technological direction and adoption addresses systems architecture, migration strategies and contingency aspects of data and system security?	RQ1, RQ2	Cloud Governance
29	How does IT process management framework addresses data and system security?	RQ1, RQ2	Cloud Governance
31	How does Enterprise IT Risk and control framework addresses issue of data and system security?	RQ1, RQ2	Cloud Governance
32	How do you educate, training and develop IT Staff for data and system security?	RQ1, RQ2	Cloud Governance
33	How do you assess quality of data and system security?	RQ1, RQ2	Cloud Governance
35	How do you protect technological infrastructure (physically) to prevent loss of data and threat to information system security?	RQ1, RQ2	Cloud Governance
36	How do you control the IT contracts of projects and operations to confirm data and systems security?	RQ1, RQ2	Cloud Governance
38	Are there any specific service level agreements (SLAs) in business usual activities that cover data and system security related aspects?	RQ1, RQ2	Cloud Governance
41	Are service desk agents are educated, trained and skilled to record, report and respond to incidents raised for data and system security breach?	RQ1, RQ2	Cloud Governance

Question No.	Question Description	Research Question (RQ) No.	Research Area
43	On the scale of 1 to 10, (10 being very complex) how complex you see monitoring and managing cloud hosted via 3rd party contractor?	RQ1, RQ2	Cloud Governance

Table 54: RQ1 and RQ2 in survey questions on cloud security

Question No.	Question Description	Research Question (RQ) No.	Research Area
32	What is the mechanism to identify malicious code injection or script run on desktops, servers, storage drives and resources on cloud?	RQ1, RQ2	Cloud Security
36	Is there a repository of antimalware identified to develop Bank's defence system secure from similar attack in future?	RQ1, RQ2	Cloud Security
41	Who is responsible for physical security of data centre?	RQ1, RQ2	Cloud Security
48	Do you see need to share information about cyber-attack or potential threat with other Banks to improve security and bring shared knowledge to a common platform?	RQ1, RQ2	Cloud Security
49	Has cloud computing added more risk to Bank?	RQ1, RQ2	Cloud Security
20	Do you have dedicated team to handle security policy compliance and incidents?	RQ1, RQ2	Cloud Security
26	What are the methods to manage Identity and access management (IAM) for cloud infrastructure?	RQ1, RQ2	Cloud Security
28	Do you have dedicated high severity incident management and response team?	RQ1, RQ2	Cloud Security
31	Is there any defined process to action against suspicious behaviour in network security perimeter? (User logging, Intrusion identification, account hijacking, password failures)	RQ1, RQ2	Cloud Security

Below shows the responses received for RQ1 and RQ2 from survey Participants:

Table 55 shows that 92 of the total survey participants and Figure 46 shows that 44.88% of participants responded that ‘Strategic plan has identified goals and methods to achieve strategic objectives of data and system security’ to assess data security and system security at management / governance forum.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 55: Strategic plan to handle data privacy and system security.

Does the business have a clear strategic plan to assess data security and system security at management / governance forum?		
User Back-ground check	**No. of Responses**	**No. of Responses as % of Total**
Yes – plan has identified goals and methods to achieve strategic objectives of data and system security	92	44.88%
Yes – there are tentative guidelines to meet data and security objective	76	37.07%
Yes – there are objectives but not explicitly mentioned in strategic plans	43	20.98%
No – there is no strategic plan and only need based activities are conducted for data and system security	38	18.54%

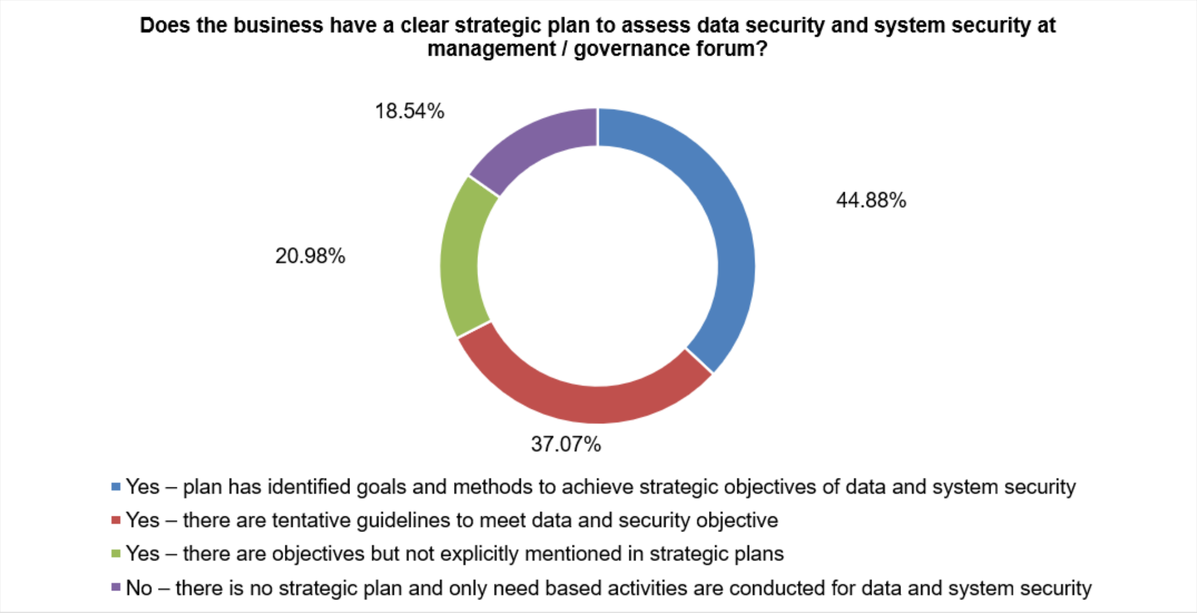


Figure 46

Table 56 shows that 79 of the total survey participants and Figure 47 shows that 38.54% of participants responded that 'PPMO considers data and security requirement as part of projects' clearly as a part of project delivery.

Table 56: New project delivery, data loss prevention and system security

Does the project portfolio management office (PPMO) clearly define, evaluate, prioritise, select, initiate, manage, and control data and system security related changes as a part of project delivery?		
Response from PPMO	**No. of Responses**	**No. of Responses as % of Total**
Yes – PPMO includes data and system security requirements	68	33.17%
Yes – PPMO considers data and security requirement as part of projects	79	38.54%
Yes – PPMO considers data and system security on need basis	57	27.80%
No – PPMO is aware of data and system security needs	27	13.17%
Unsure / don't know	38	18.54%
Total	**205**	**100.00%**

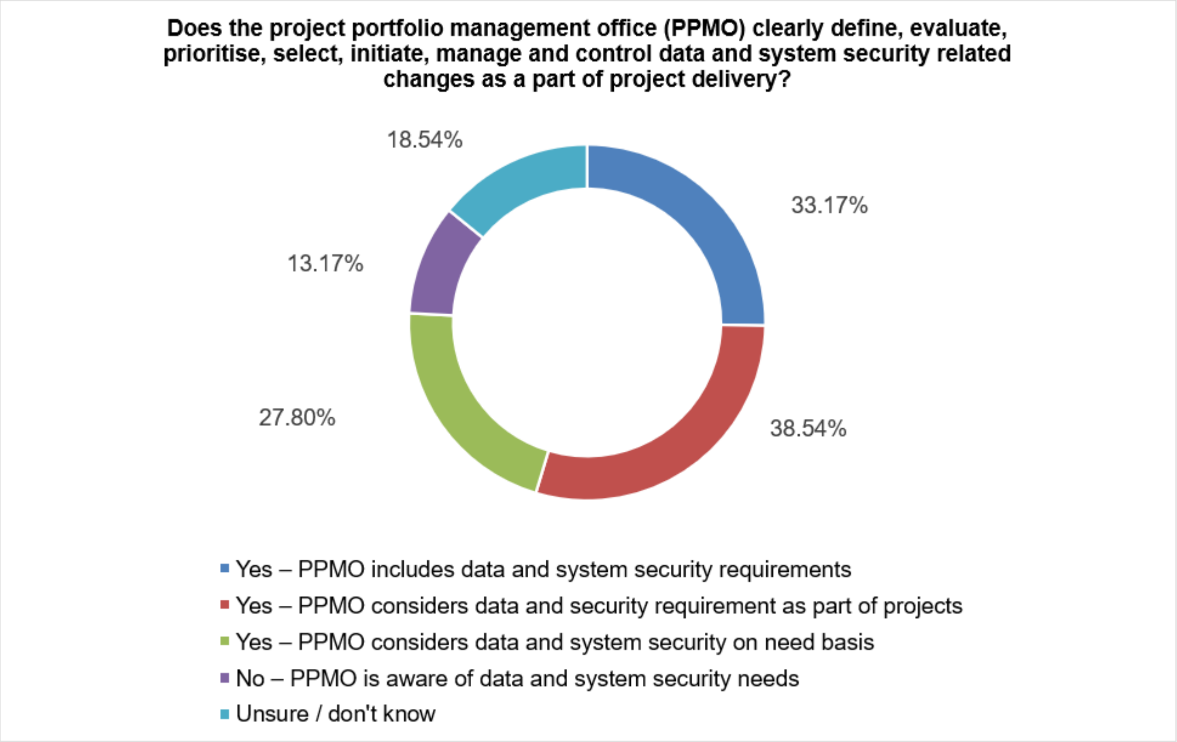

Does the project portfolio management office (PPMO) clearly define, evaluate, prioritise, select, initiate, manage and control data and system security related changes as a part of project delivery?
18.54%
33.17%
13.17%
27.80%
38.54%
■ Yes – PPMO includes data and system security requirements
■ Yes – PPMO considers data and security requirement as part of projects
■ Yes – PPMO considers data and system security on need basis
■ No – PPMO is aware of data and system security needs
■ Unsure / don't know

Figure 47

Table 57 shows that 110 of the total survey participants and Figure 48 shows that 53.66% of participants responded that ‘Regular data backup jobs, Data warehouse reporting, DR server storage and change management process governs data integrity’.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 57: Data integrity on cloud

How does the business manage the integrity of data stored in electronic form such as, databases, data warehouse and data archives?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Regular data backup jobs, Data warehouse reporting, DR server storage and change management process governs data integrity	110	53.66%
Data Backup and archival job run weekly / monthly basis to secure data. Data integrity is with respective departments	88	42.93%
Data backup and data integrity are with IT department and no involvement of governance forum	65	31.71%
No control or process for data integrity and data backup unless need arises	16	7.80%

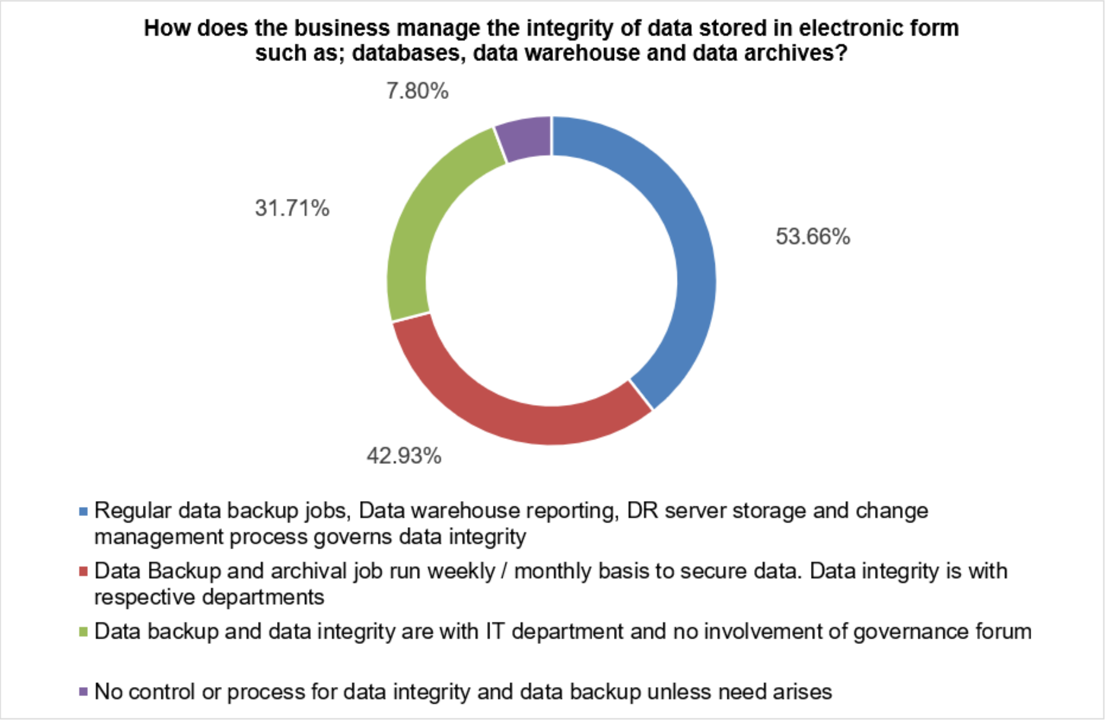

How does the business manage the integrity of data stored in electronic form such as; databases, data warehouse and data archives?
7.80%
31.71%
53.66%
42.93%
■ Regular data backup jobs, Data warehouse reporting, DR server storage and change management process governs data integrity
■ Data Backup and archival job run weekly / monthly basis to secure data. Data integrity is with respective departments
■ Data backup and data integrity are with IT department and no involvement of governance forum
■ No control or process for data integrity and data backup unless need arises

Figure 48

Table 58 shows that 105 of the total survey participants and Figure 49 shows that 51.22% of participants responded that ‘data and system security are key parameters to evaluate adoption and upgrade of technology’.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 58: Technology adoption and IT infrastructure

Does technological direction and adoption address system architecture, migration strategies and contingency aspects of data and system security?		
Technological Direction	**No. of Responses**	**No. of Responses as % of Total**
Yes – data and system security are key parameters to evaluate adoption and upgrade of technology	105	51.22%
Yes – Data and system security aspects are considered, however, not a priority	71	34.63%
Yes – Data and systems security are considered only if adoption of technology directly affects them	49	23.90%
No – Data and system security are not considered under the assumption that new technology will automatically consider it	28	13.66%

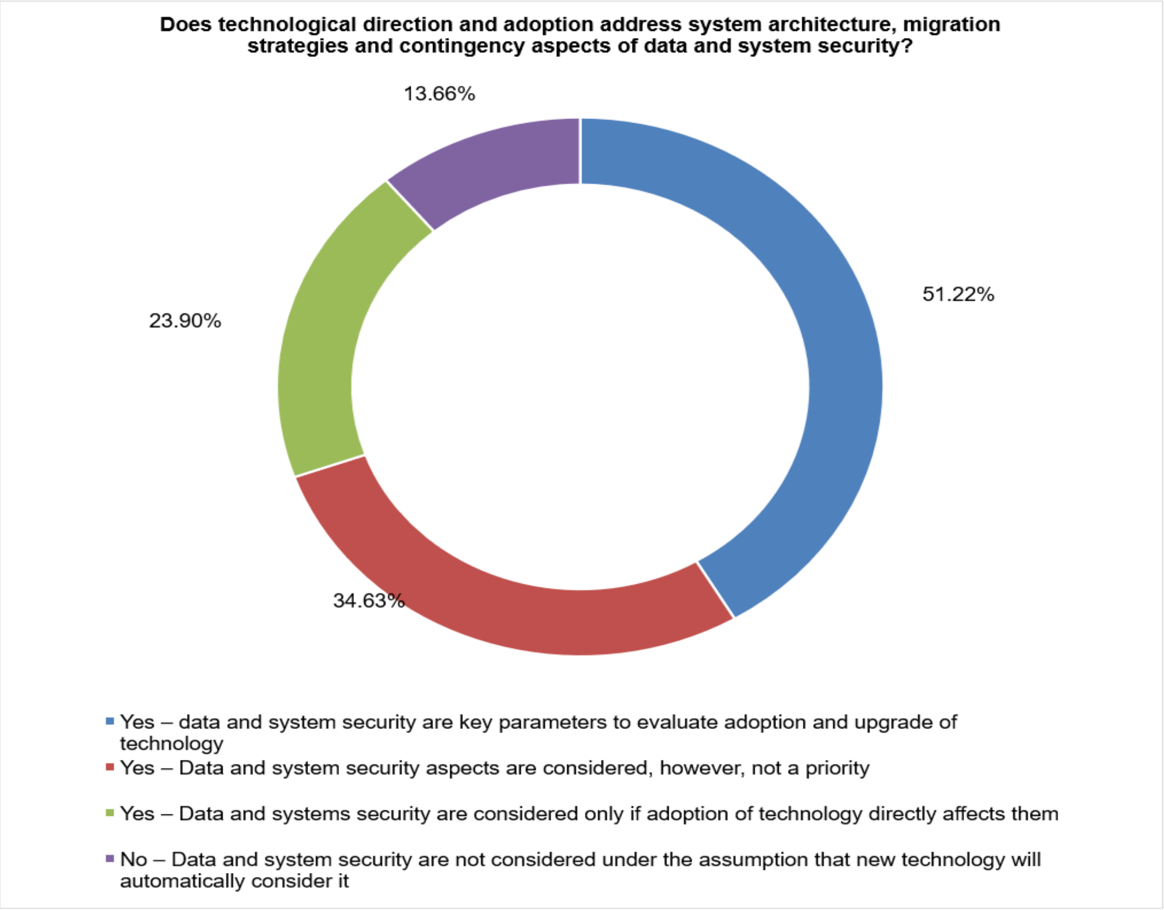

Does technological direction and adoption address system architecture, migration strategies and contingency aspects of data and system security?
13.66%
51.22%
23.90%
34.63%
🟦 Yes – data and system security are key parameters to evaluate adoption and upgrade of technology
🟥 Yes – Data and system security aspects are considered, however, not a priority
🟩 Yes – Data and systems security are considered only if adoption of technology directly affects them
🟪 No – Data and system security are not considered under the assumption that new technology will automatically consider it

Figure 49

Table 59 shows that 99 of the total survey participants and Figure 50 shows that 48.29% of participants responded that ‘IT Process Management defines methods to add, modify, remove data and system security configuration through change and release management process’.

Table 59: IT processes, data & system security

How does the company’s IT process management framework address data and system security?		
IT Processes	**No. of Responses**	**No. of Responses as % of Total**
IT Process Management defines methods to add, modify, remove data and system security configuration through change and release management process	99	48.29%
IT Process Management provides guidelines to manage data and security, however, does not provide methods to maintain data and security configuration	83	40.49%
IT Process Management does not deal with data and system security related processes	23	11.22%
Total	**205**	**100.00%**

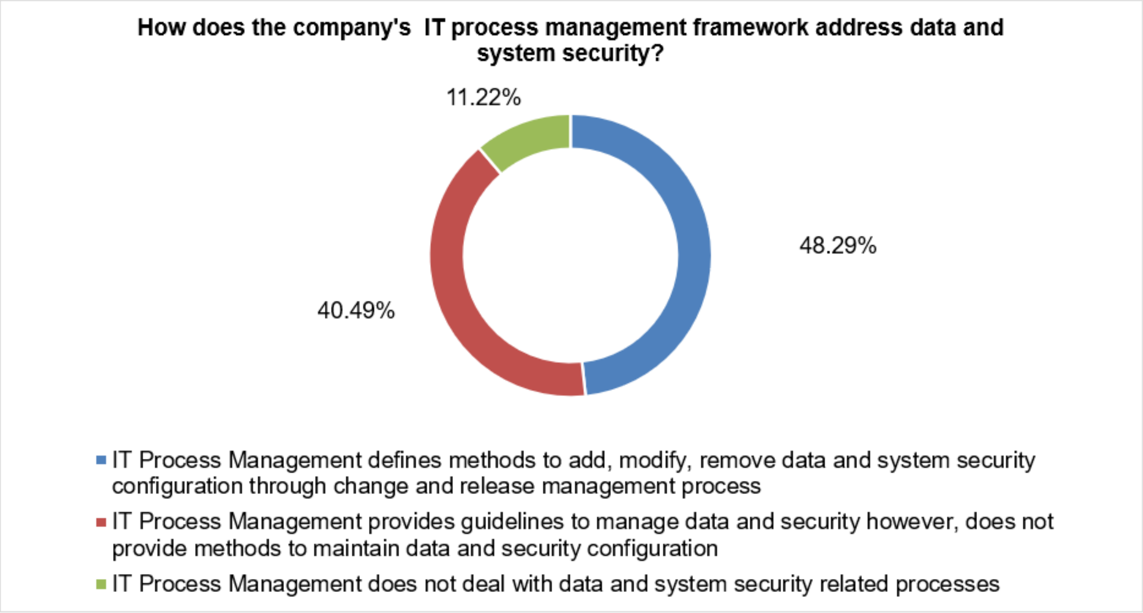


Figure 50

Table 60 shows that 75 of the total survey participants and Figure 51 shows that 36.59% of participants responded that ‘IT Risk and Control framework sets clear guidelines, assesses, advises, and helps to maintain data and system security related aspects in IT’ followed by ‘IT Risk and Control framework provides high level guidelines to be followed to secure data and system security’.

Table 60: IT risk, data & system security

How does the business IT Risk and control framework address issues for data and system security?		
IT Risk	**No. of Responses**	**No. of Responses as % of Total**
IT Risk and Control framework sets clear guidelines, assesses, advises, and helps to maintain data and system security related aspects in IT	75	36.59%
IT Risk and Control framework provides high level guidelines to be followed to secure data and system security	74	36.10%
IT Risk and Control Framework loosely connects with data and system security framework	41	20.00%
IT Risk and Control framework does not provide any guidelines to data and system security	15	7.32%
Total	**205**	**100.00%**

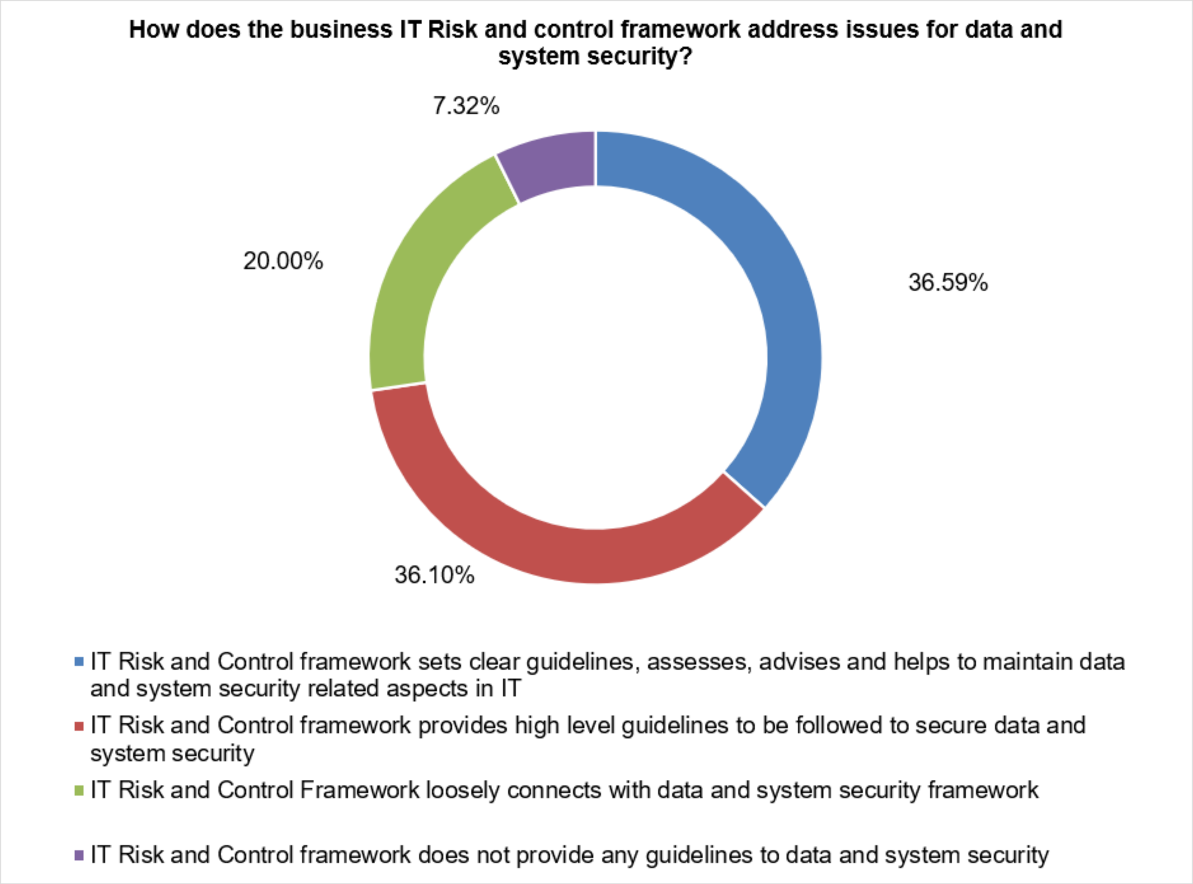

How does the business IT Risk and control framework address issues for data and system security?
7.32%
20.00%
36.59%
36.10%
■ IT Risk and Control framework sets clear guidelines, assesses, advises and helps to maintain data and system security related aspects in IT
■ IT Risk and Control framework provides high level guidelines to be followed to secure data and system security
■ IT Risk and Control Framework loosely connects with data and system security framework
■ IT Risk and Control framework does not provide any guidelines to data and system security

Figure 51

Table 61 shows that 75 of the total survey participants and Figure 52 shows that 36.59% of participants responded that ‘There is mandatory general training and information modules which provide details to employees about data and system security’ to educate, train, and develop IT Staff on data and system security’.

Table 61: IT training, data & system security

How does the business educate, train, and develop IT Staff on data and system security?		
IT Training	**No. of Responses**	**No. of Responses as % of Total**
There is mandatory comprehensive training module dedicated for data and system security for each employee which gets updated with needs of the business environment	48	23.41%
There is mandatory general training and information modules which provide details to employees about data and system security	75	36.59%
There is general guidelines for each employee to meet data and system security standards	39	19.02%
There is a general guidelines and option training module for employees for data and system security	17	8.29%
There are no training plans for data and system security for system users	26	12.68%
Total	**205**	**100.00%**

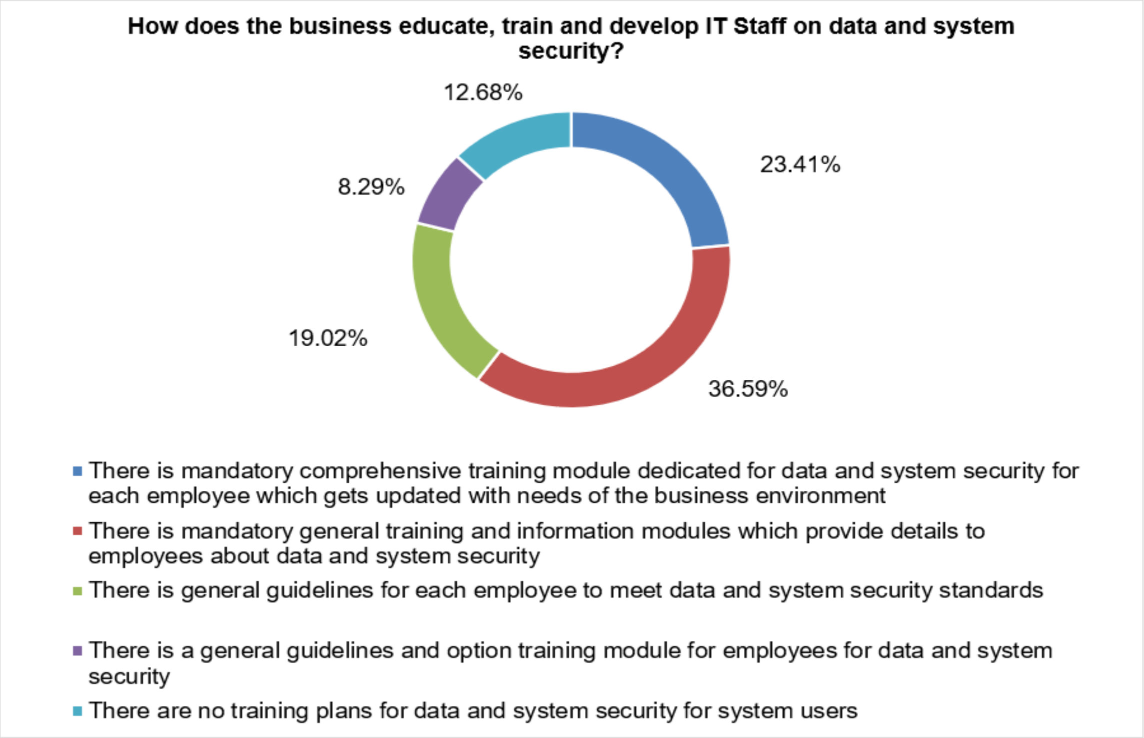

How does the business educate, train and develop IT Staff on data and system security?
12.68%
23.41%
8.29%
19.02%
36.59%
▪ There is mandatory comprehensive training module dedicated for data and system security for each employee which gets updated with needs of the business environment
▪ There is mandatory general training and information modules which provide details to employees about data and system security
▪ There is general guidelines for each employee to meet data and system security standards
▪ There is a general guidelines and option training module for employees for data and system security
▪ There are no training plans for data and system security for system users

Figure 52

Table 62 shows that 73 of the total survey participants and Figure 53 shows that 35.61% of participants responded that ‘Static and Dynamic data for application, server and security tools are configured to meet desired functionality and objectives. This is controlled at initial project level before converted to business-as-usual activity. The change in data is monitored through change and release management IT processes’ is the method to assess quality of data and system security.

Table 62: Quality control, data & system security

How does the business assess quality of data and system security?		
Quality Control	**No. of Responses**	**No. of Responses as % of Total**
Static and Dynamic data for application, server and security tools are configured to meet desired functionality and objectives. This is controlled at initial project level before converted to business-as-usual activity. The change in data is monitored through change and release management IT processes	73	35.61%
Static and Dynamic data controlled and operated by project teams. Once the data is business as usual requirements, there is no need to assess, monitor and control	69	33.66%
Static and dynamic data is managed on need basis and there are no quality control parameters	35	17.07%
There are no quality control parameters within IT Management / Governance and quality related aspects are responsibility of 3rd Party vendor supporting applications	28	13.66%
Total	**205**	**100.00%**

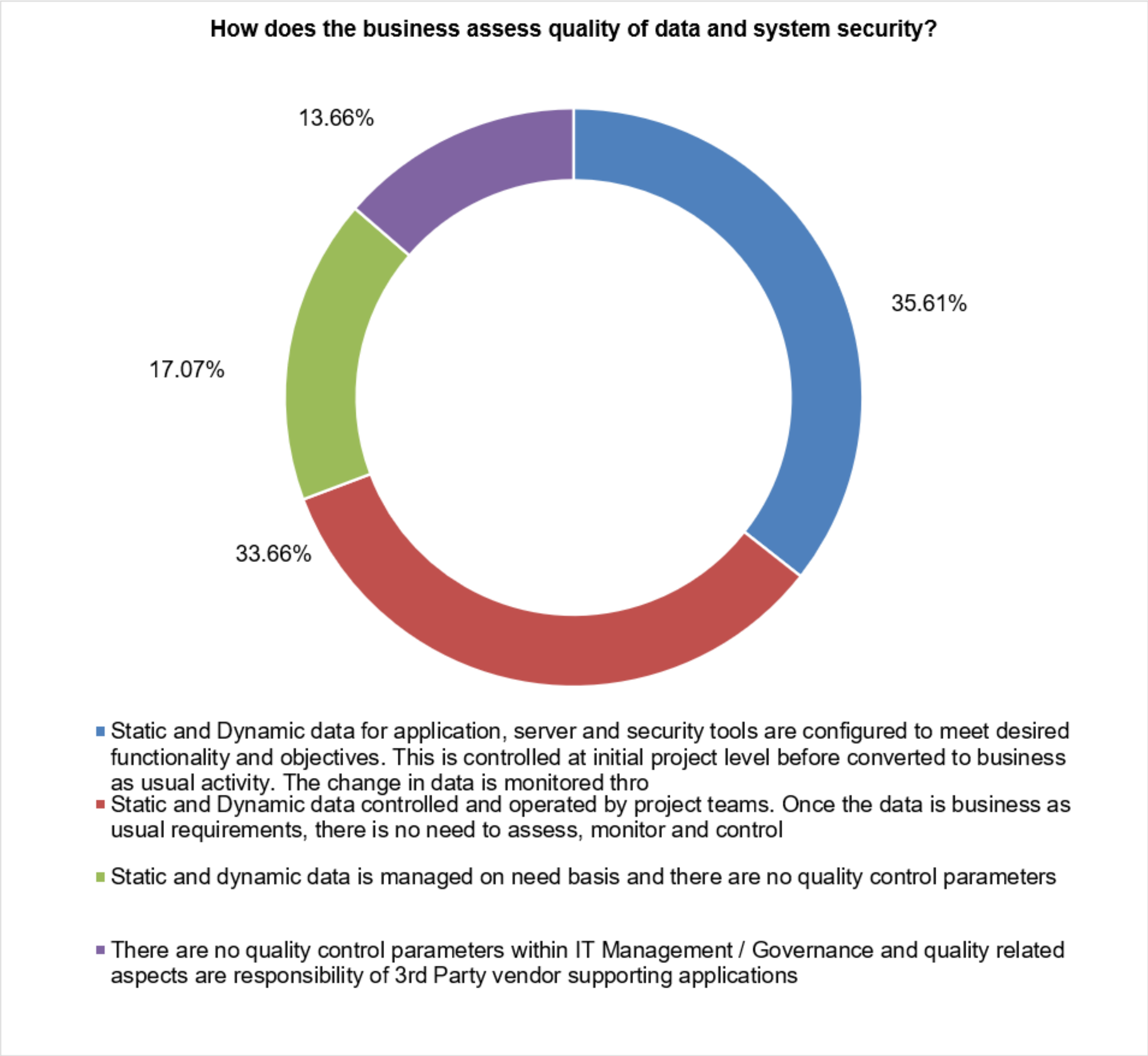

How does the business assess quality of data and system security?
13.66%
35.61%
17.07%
33.66%
🟦 Static and Dynamic data for application, server and security tools are configured to meet desired functionality and objectives. This is controlled at initial project level before converted to business as usual activity. The change in data is monitored thro
🟥 Static and Dynamic data controlled and operated by project teams. Once the data is business as usual requirements, there is no need to assess, monitor and control
🟩 Static and dynamic data is managed on need basis and there are no quality control parameters
🟪 There are no quality control parameters within IT Management / Governance and quality related aspects are responsibility of 3rd Party vendor supporting applications

Figure 53

Table 63 shows that 84 of the total survey participants and Figure 54 shows that 40.98% of participants responded that ‘The data centres are located within the company's head office with restricted access and secured by onsite security personnel’ and this helps business to protect technological infrastructure (physically) from loss of data and threats to information system security.

Table 63: Physical infrastructure protection, data & system security

How does the business protect technological infrastructure (physically) to prevent loss of data and threats to information system security?		
Quality Control	**No. of Responses**	**No. of Responses as % of Total**
The data centre (DC) is managed by 3rd party cloud service provider who manages two different data centres (Main DC and disaster recovery site)	47	22.93%
The data centres are located within the company's head office with restricted access and secured by onsite security personnel	84	40.98%
The data centres are secured by 3rd Party security services managed by cloud service provider	52	25.37%
The data centres are secured by 3rd Party security services managed by the company	22	10.73%
Total	**205**	**100.00%**

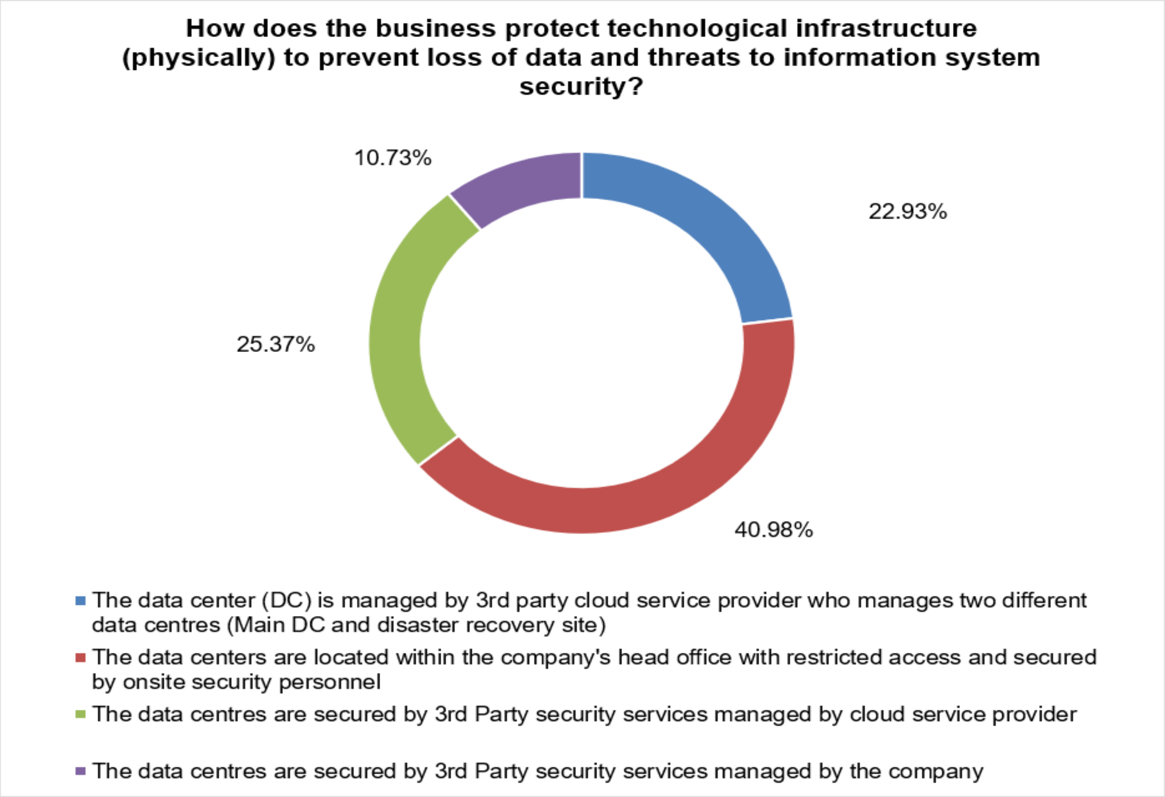

How does the business protect technological infrastructure (physically) to prevent loss of data and threats to information system security?
10.73%
22.93%
25.37%
40.98%
🟦 The data center (DC) is managed by 3rd party cloud service provider who manages two different data centres (Main DC and disaster recovery site)
🟥 The data centers are located within the company's head office with restricted access and secured by onsite security personnel
🟩 The data centres are secured by 3rd Party security services managed by cloud service provider
🟪 The data centres are secured by 3rd Party security services managed by the company

Figure 54

Table 64 shows that 68 of the total survey participants and Figure 55 shows that 33.17% of participants responded that ‘IT Contracts are developed in specific clauses for data and system security and are present in each contract signed with 3rd Party contractors and IT Service providers’ and this helps business to control the IT contracts of projects and operations to confirm data and systems security.

Table 64: IT contracts, data & system security

How does the business control the IT contracts of projects and operations to confirm data and systems security?		
IT Contracts	**No. of Responses**	**No. of Responses as % of Total**
IT Contracts are developed in specific clauses for data and system security and are present in each contract signed with 3rd Party contractors and IT Service providers	68	33.17%
IT contracts include Data and system security clauses on a need basis	48	23.41%
All IT contracts include general clauses data and system security	50	24.39%
IT Contracts do not include data and security clauses	14	6.83%
Unsure / Don't know	25	12.20%
Total	**205**	**100.00%**

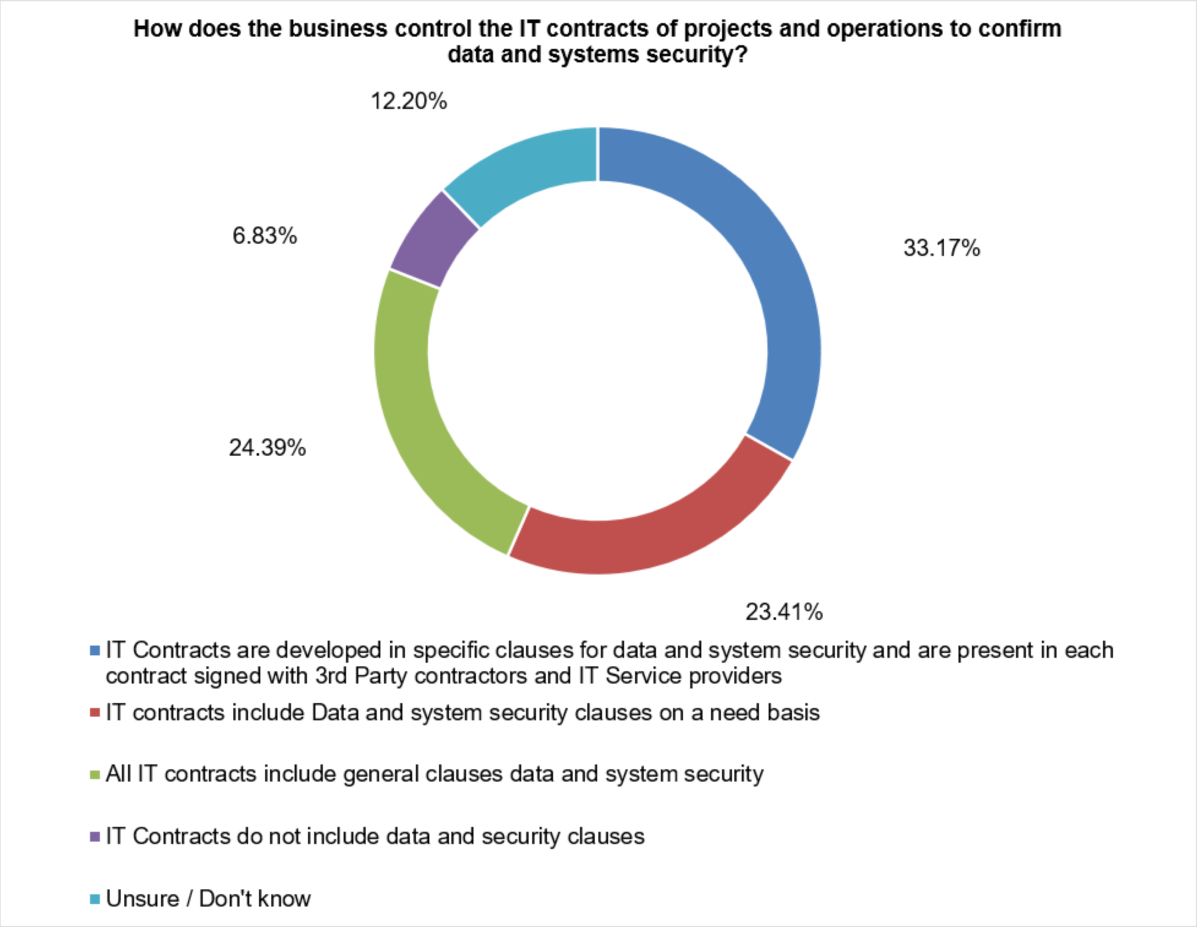

How does the business control the IT contracts of projects and operations to confirm data and systems security?
12.20%
6.83%
33.17%
24.39%
23.41%
■ IT Contracts are developed in specific clauses for data and system security and are present in each contract signed with 3rd Party contractors and IT Service providers
■ IT contracts include Data and system security clauses on a need basis
■ All IT contracts include general clauses data and system security
■ IT Contracts do not include data and security clauses
■ Unsure / Don't know

Figure 55

Table 65 shows that 104 of the total survey participants and Figure 56 shows that 50.73% of participants responded that ‘All Data and system security related incidents are marked high impact and high risk and follow strict SLA adherence’ and this is the method to enforce Service Level Agreements (SLAs) in the businesses usual activities that cover data and system security related aspects.

Table 65: Service level agreements, data & system security

Are there any specific Service Level Agreements (SLAs) in the businesses usual activities that cover data and system security related aspects?		
Service Level Agreements	**No. of Responses**	**No. of Responses as % of Total**
Yes – All Data and system security related incidents are marked high impact and high risk, and follow strict SLA adherence	104	50.73%
No – SLAs do not consider impact to Data and system security	42	20.49%
Yes – Data and System security related aspects are considered while following SLAs however, they are not given priority	43	20.98%
Data and system security related aspects are not important for SLAs definition	16	7.80%
Total	**205**	**100.00%**

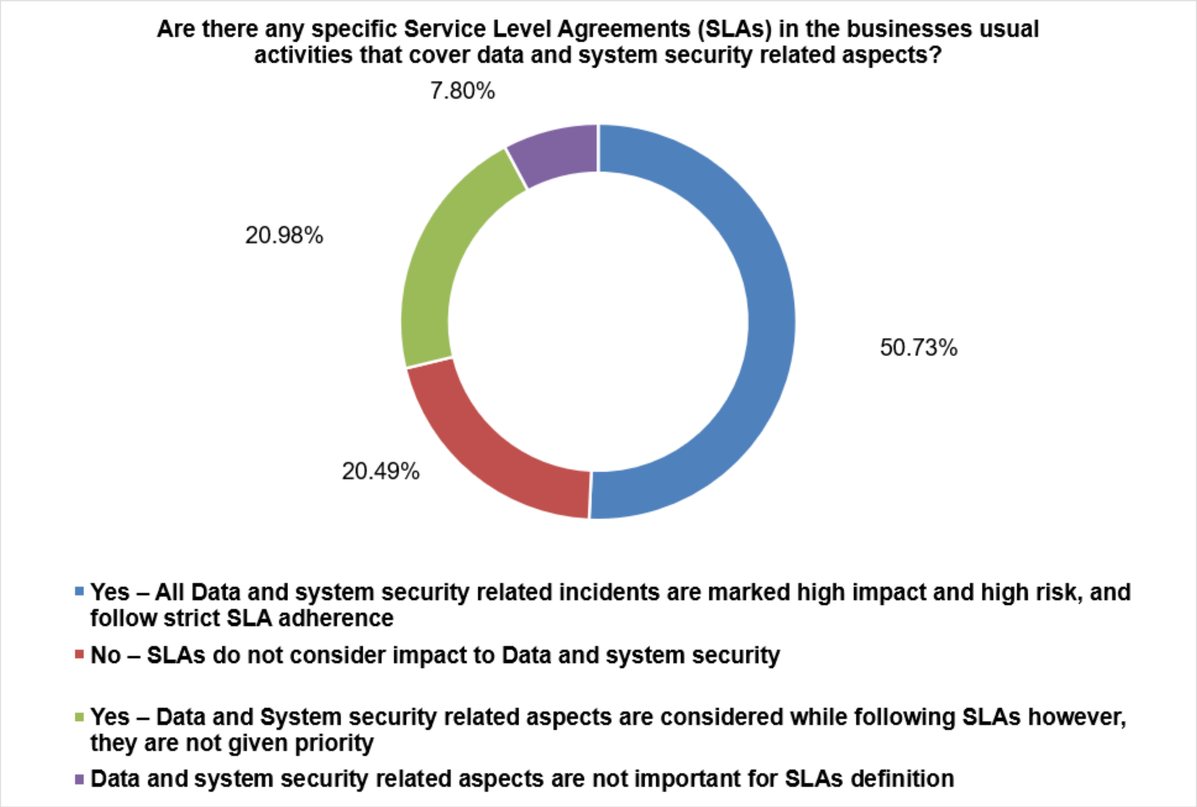

Are there any specific Service Level Agreements (SLAs) in the businesses usual activities that cover data and system security related aspects?
7.80%
20.98%
50.73%
20.49%
Yes – All Data and system security related incidents are marked high impact and high risk, and follow strict SLA adherence
No – SLAs do not consider impact to Data and system security
Yes – Data and System security related aspects are considered while following SLAs however, they are not given priority
Data and system security related aspects are not important for SLAs definition

Figure 56

Table 66 shows that 79 of the total survey participants and Figure 57 shows that 38.54% of participants responded that ‘Service desk agents are made aware of data and system security related incidents’ and this helps to report and respond to incidents raised for data and system security breach(s).

Table 66: Service desk education, data & system security

Are service desk agents educated, trained and skilled to record, report and respond to incidents raised for data and system security breach(s)?		
Service Desk Education	**No. of Responses**	**No. of Responses as % of Total**
Yes – Service desk agents are provided separate guidelines and SLAs to handle data and system security breach related incidents	71	34.63%
Yes – Service desk agents are made aware of data and system security related incidents	79	38.54%
No – Service desk agents classify incident in general and do not pay specific importance to data and system security related incidents	32	15.61%
No – Service desk agents are only to record incidents and classification based on data and system security is handled by a separate team	23	11.22%
Total	**205**	**100.00%**

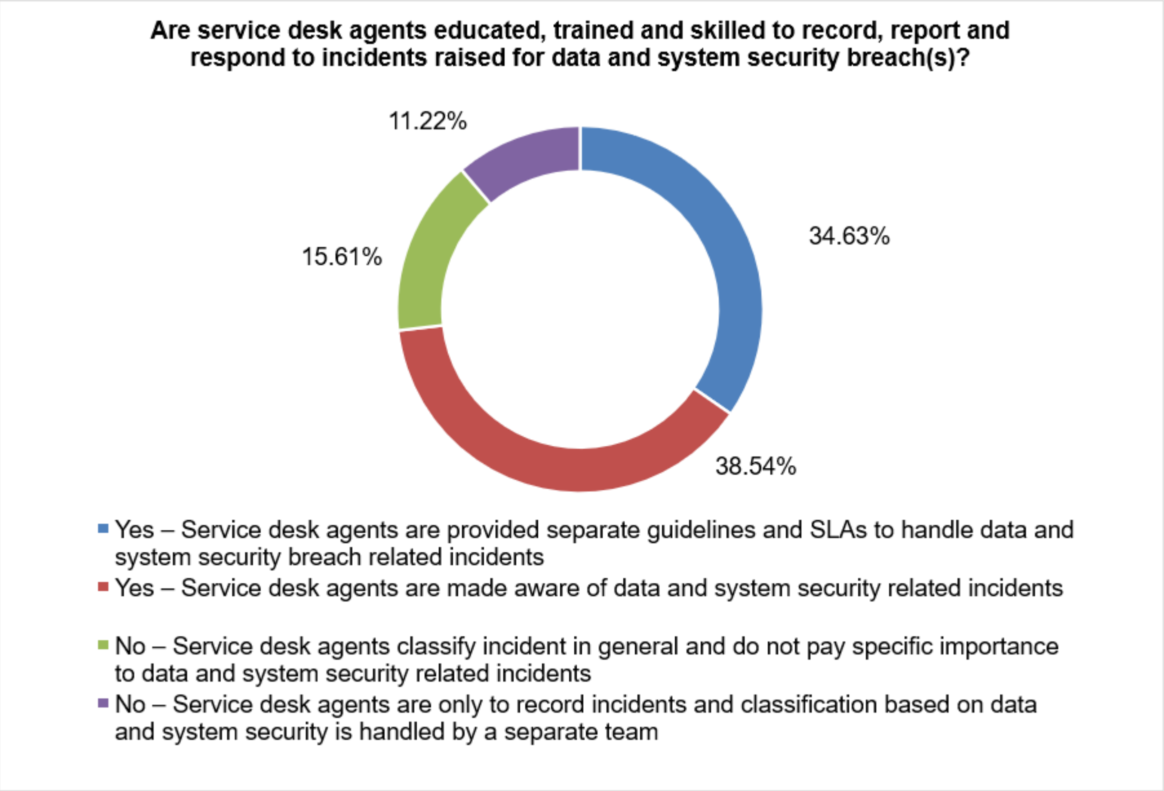


Figure 57

Table 67 shows that 51 of the total survey participants and Figure 58 shows that 24.88% of participants responded that it is very complex to monitor and manage IT infrastructure (Cloud) hosted via 3rd party contractor.

Table 67: Complexity to manage IT infrastructure on cloud

On the scale of 1 to 10, (1 being not at all complex and 10 being very complex) how complex do you see monitoring and managing IT infrastructure (Cloud) hosted via 3rd party contractor?		
Complexity to Manage Cloud	**No. of Responses**	**No. of Responses as % of Total**
1 - Not at all complex	1	0.49%
2	2	0.98%
3	5	2.44%
4	7	3.41%
5	19	9.27%
6	35	17.07%
7	51	24.88%
8	46	22.44%
9	23	11.22%
10 - very complex	16	7.80%
Total	**205**	**100.00%**

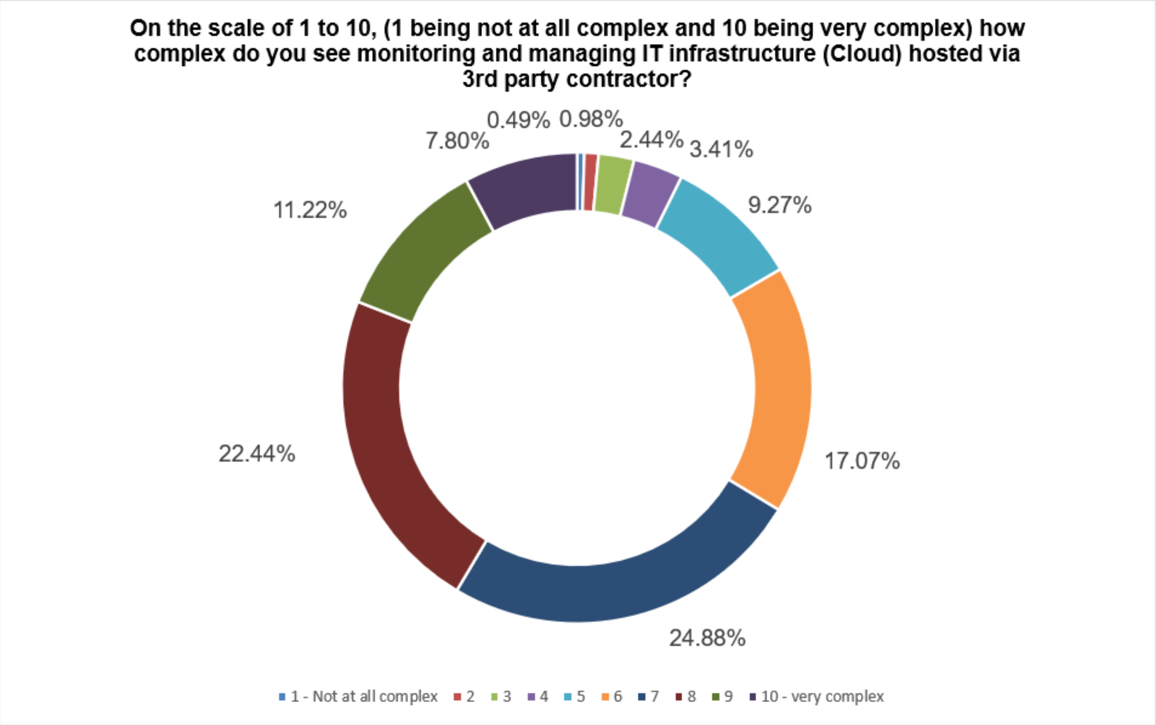

On the scale of 1 to 10, (1 being not at all complex and 10 being very complex) how complex do you see monitoring and managing IT infrastructure (Cloud) hosted via 3rd party contractor?
0.49%
0.98%
2.44%
3.41%
9.27%
17.07%
24.88%
22.44%
11.22%
7.80%
1 - Not at all complex
2
3
4
5
6
7
8
9
10 - very complex

Figure 58

Table 68 shows that 105 of the total survey participants and Figure 59 shows that 51.22% of participants responded that ‘Monitoring and Alert Mechanism run in real time to identify and quarantine malicious scripts / codes / .exe files’ to identify malicious code injection or script run on desktops, servers, storage drives and resources on IT Infrastructure (Cloud).

Table 68: Virus attack and security of IT infrastructure on cloud

What is the mechanism used to identify malicious code injection or script run on desktops, servers, storage drives and resources on IT Infrastructure (Cloud)?		
Virus Injection	**No. of Responses**	**No. of Responses as % of Total**
No scripts / codes / .exe files can be developed and run on internal systems	55	26.83%
Development of codes / scripts and deploying them over cloud environments is task by dedicated team through system change approval process	93	45.37%
Monitoring and Alert Mechanism run in real time to identify and quarantine malicious scripts / codes / .exe files	105	51.22%
System configuration prevents development and deployment of scripts / codes / .exe files	64	31.22%
Total	**205**	**100.00%**

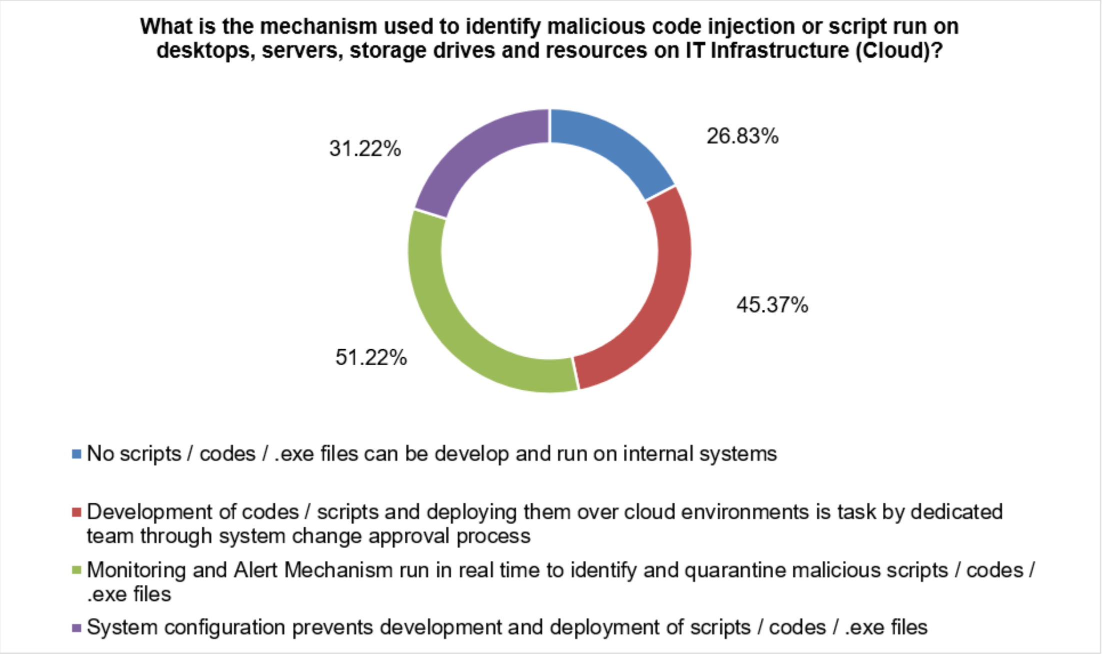


Figure 59

Table 69 shows that 104 of the total survey participants and Figure 60 shows that 50.73% of participants responded that 'Anti-Malware engine keep records of all identified threat and provides detection and protection' to keep repository of antimalware identified to develop Company's defence system secure from similar attacks in the future.

Table 69: Antimalware and security of IT infrastructure on cloud

Is there a repository of antimalware identified to develop Company's defence system secure from similar attacks in the future?		
Antimalware	**No. of Responses**	**No. of Responses as % of Total**
Yes – Anti-Malware engine keep records of all identified threat and provides detection and protection	104	50.73%
Yes – Limited information can be stored about type of attacks but prevention depends on available defence mechanism	59	28.78%
No – There is no mechanism to store and retain malware	42	20.49%
Total	**205**	**100.00%**

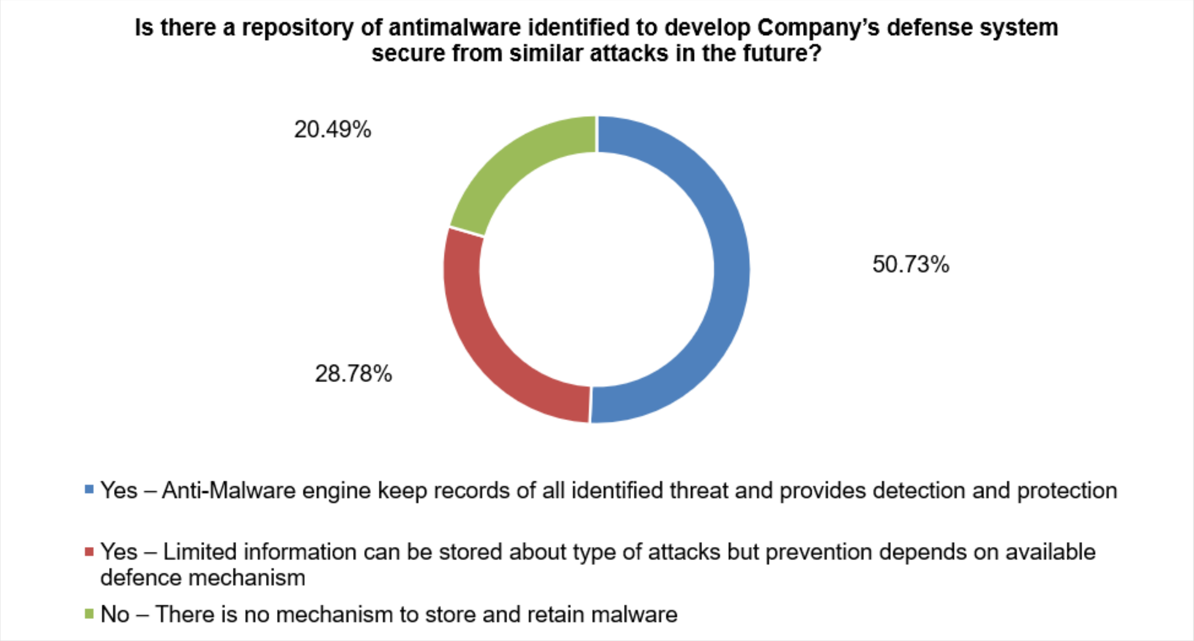


Figure 60

Table 70 shows that 90 of the total survey participants and Figure 61 shows that 43.90% of participants responded that ‘The Company’ is responsible for physical security of data centre.

Table 70: Security of data centre and security of IT infrastructure on cloud

Who is responsible for physical security of data centre?		
Responsible Entity	**No. of Responses**	**No. of Responses as % of Total**
The Company	90	43.90%
IT Infrastructure (Cloud) Service provider (Amazon (AWS), Microsoft Azure, Google Cloud etc.)	82	40.00%
3rd Party Security Services	33	16.10%
Total	**205**	**100.00%**

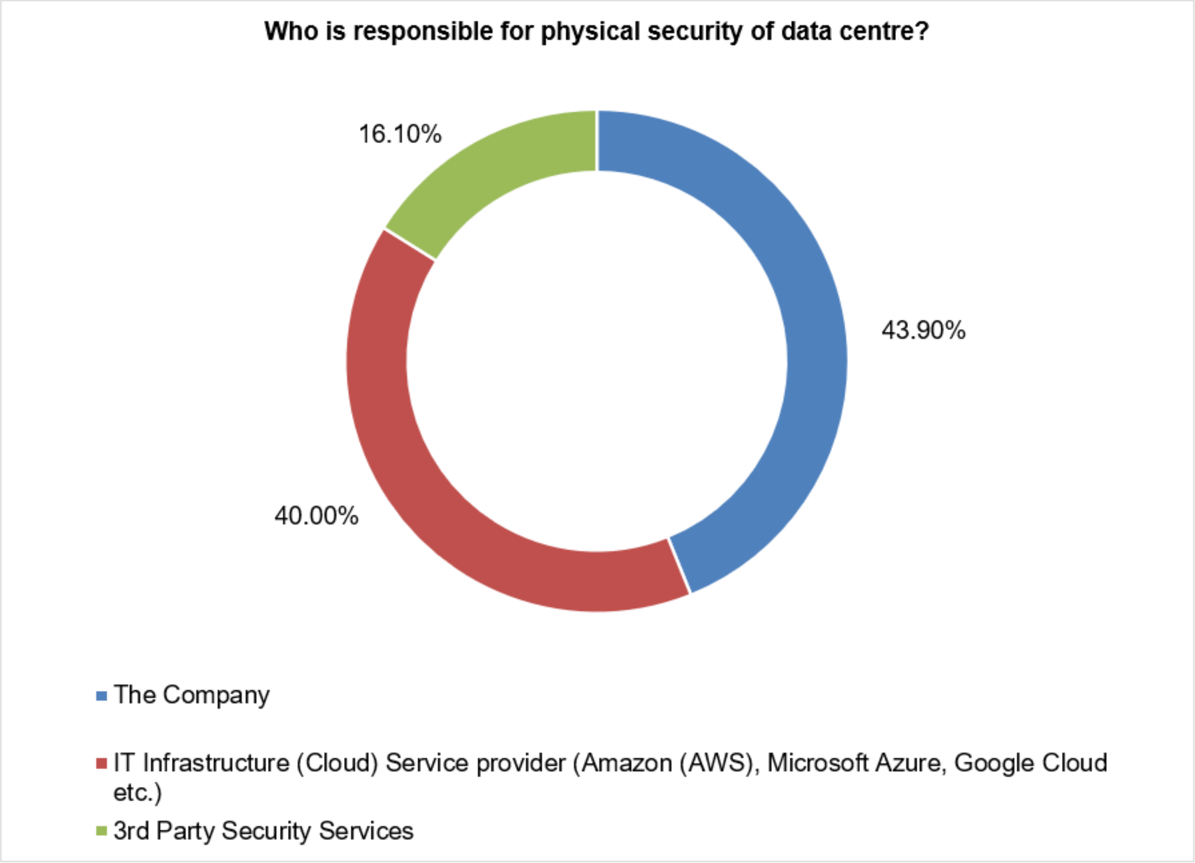


Figure 61

Table 71 shows that 107 of the total survey participants and Figure 62 shows that 52.20% of participants responded that sharing information about cyber-attacks or potential threats with other companies will improve monitoring and response to security incidents.

Table 71: Common knowledge platform for security of IT infrastructure on cloud

Do you see a need to share information about cyber-attacks or potential threats with other companies to improve security and bring shared knowledge to a common platform?		
Information Sharing	**No. of Responses**	**No. of Responses as % of Total**
Yes – this will improve monitoring and response to security incidents	107	52.20%
No – This may lead to breach of organization policy	69	33.66%
Not Required as there are several public forums who are providing same platform	29	14.15%
Total	**205**	**100.00%**

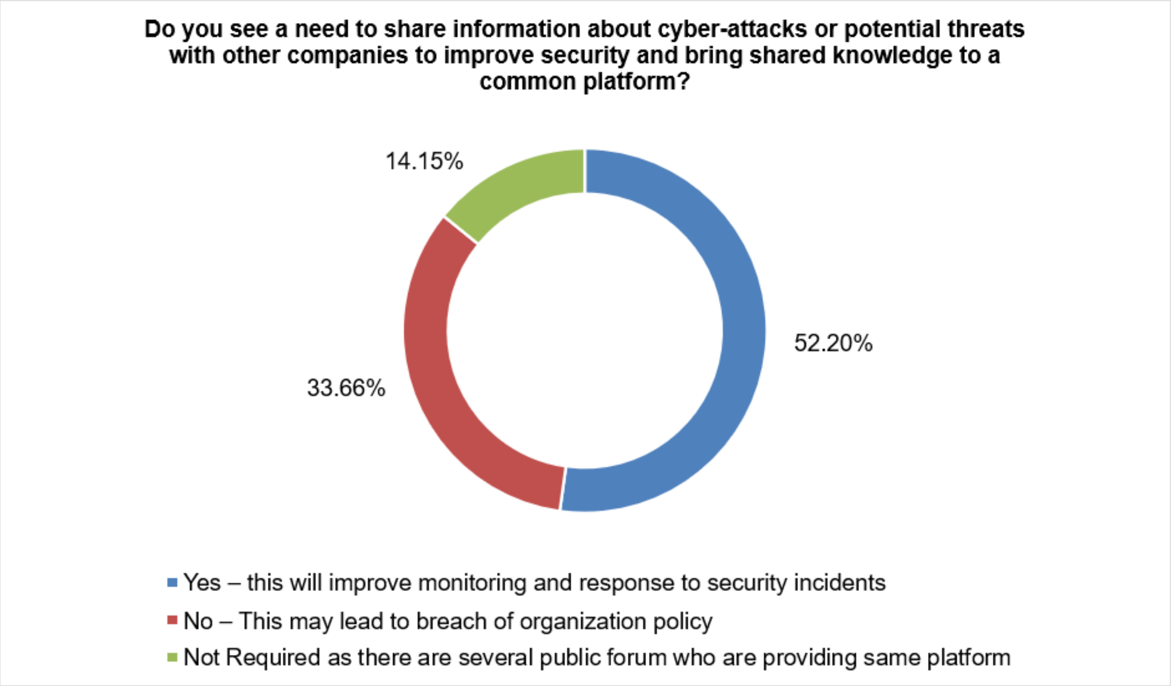


Figure 62

Table 72 shows that 90 of the total survey participants and Figure 63 shows that 43.90% of participants responded that ‘Cloud Computing has added new risk areas to IT infrastructure’, followed by ‘more task and failure to which led to further risk’.

Table 72: Risk level of IT infrastructure on cloud

Has IT Infrastructure (Cloud) computing added more risk to the company?		
Risk Level	**No. of Responses**	**No. of Responses as % of Total**
Yes – It added more task and failure to which led to further risk	52	25.37%
Yes – It has created new risk areas	90	43.90%
No – Cloud computing is safe	39	19.02%
It is safe until it is maintained well	24	11.71%
Total	**205**	**100.00%**

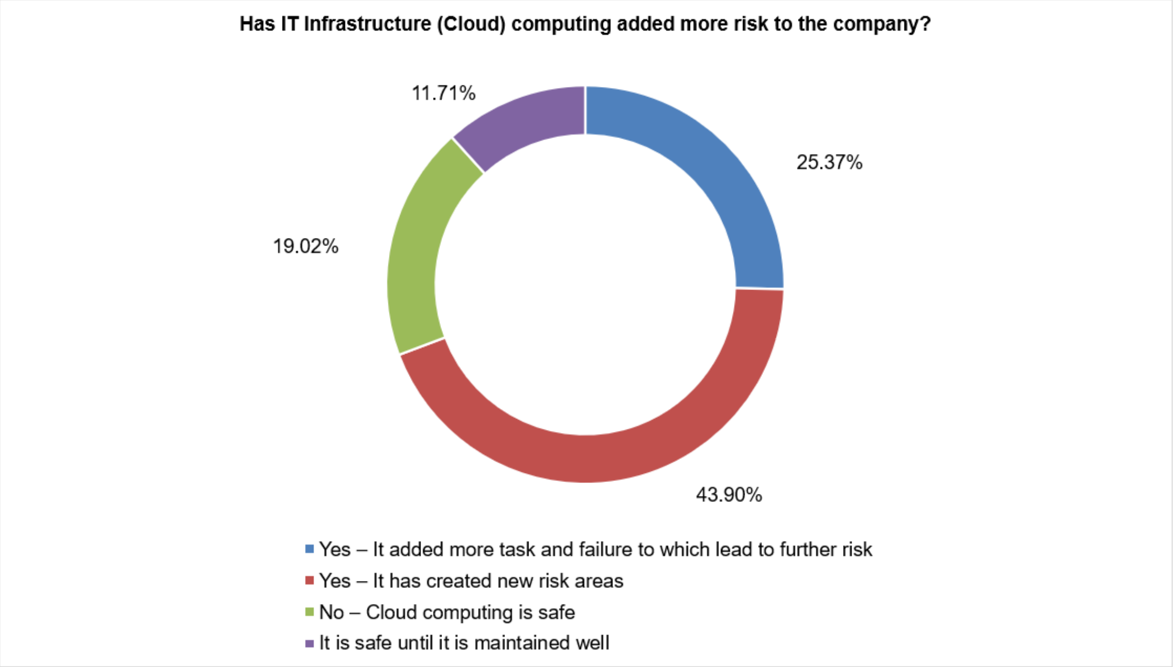


Figure 63

Table 73 shows that 64 of the total survey participants and Figure 64 shows that 31.22% of participants responded that ‘Dedicated Expert team to respond to risk events’, followed by ‘Regular Team to handle events’ in the event to work on high severity security incident.

Table 73: Policy and compliance incident and IT support team

Does the business have a dedicated high severity security incident management and response team?		
Dedicated IT Support Teams	**No. of Responses**	**No. of Responses as % of Total**
Yes – Dedicated Expert team to respond to risk events	64	31.22%
Fairly Mature team	34	16.59%
Regular Team to handle events	61	29.76%
Team Development on need basis	46	22.44%
Total	**205**	**100.00%**

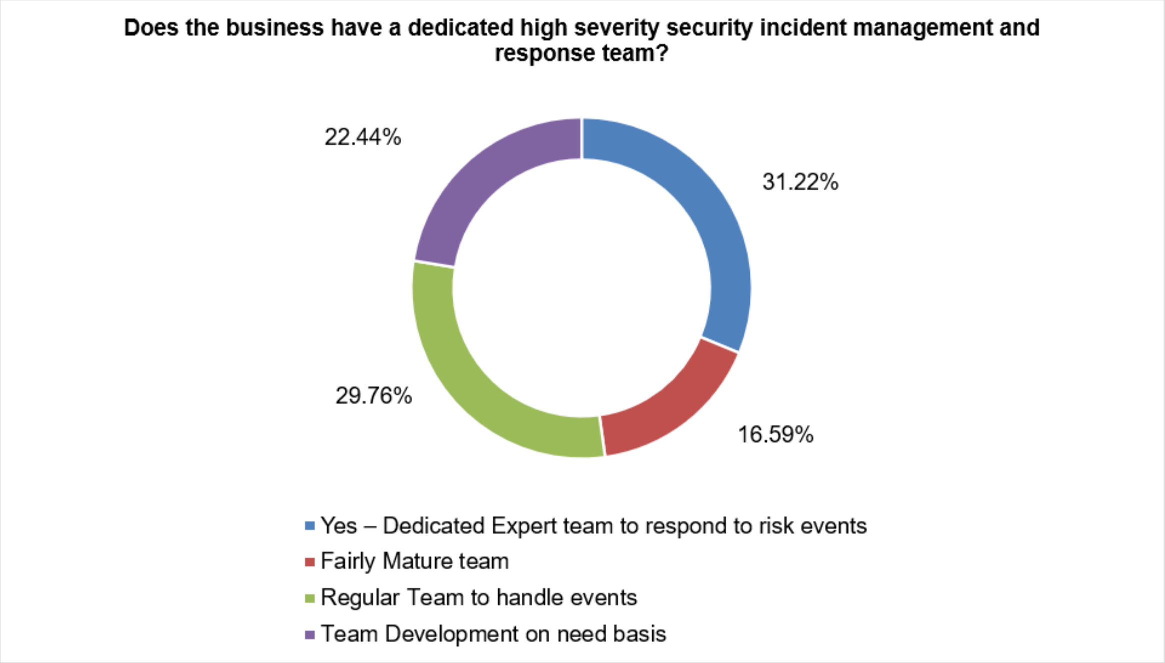


Figure 64

Table 74 shows that 72 of the total survey participants and Figure 65 shows that 35.12% of participants responded that ‘Identity and Access Management (IAM) Tools’ are used to manage Identity and access management (IAM) for IT Infrastructure.

Table 74: IAM and IT infrastructure (cloud)

What are the methods used to manage Identity and access management (IAM) for IT Infrastructure?		
IAM Tools	**No. of Responses**	**No. of Responses as % of Total**
Identity and Access Management (IAM) Tools	72	35.12%
Manual Process	34	16.59%
Automated Checks and Manual removal of User ids	51	24.88%
Need based process	48	23.41%
Total	**205**	**100.00%**

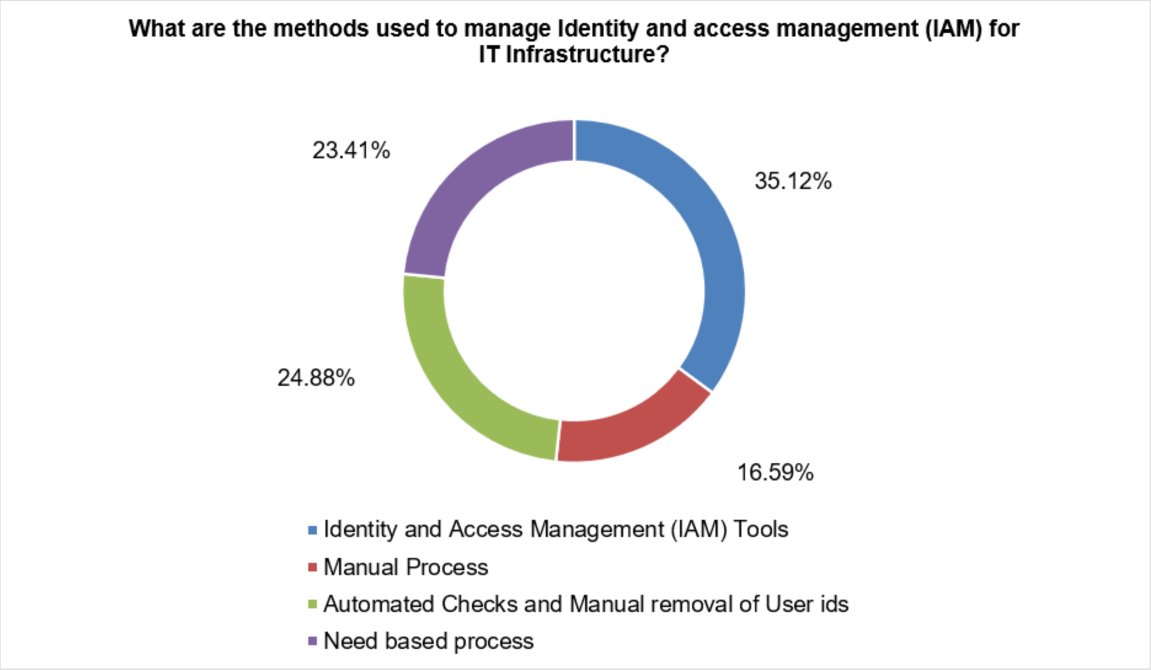


Figure 65

Table 75 shows that 89 of the total survey participants and Figure 66 shows that 43.41% of participants responded that ‘Advance tools, communication channel and action items in place’ to action against suspicious behaviour in network security perimeter.

Table 75: High severity incident management team and IT infrastructure (cloud)

Is there any defined process to action against suspicious behaviour in network security perimeter? (User logging, Intrusion identification, account hijacking, password failures)		
Dedicated IT Support Teams for High Severity Incidents	**No. of Responses**	**No. of Responses as % of Total**
Yes – Advance tools, communication channel and action items in place	89	43.41%
Yes – Process in place only for few identified events	63	30.73%
No process in place and actions are need based	53	25.85%
Total	**205**	**100.00%**

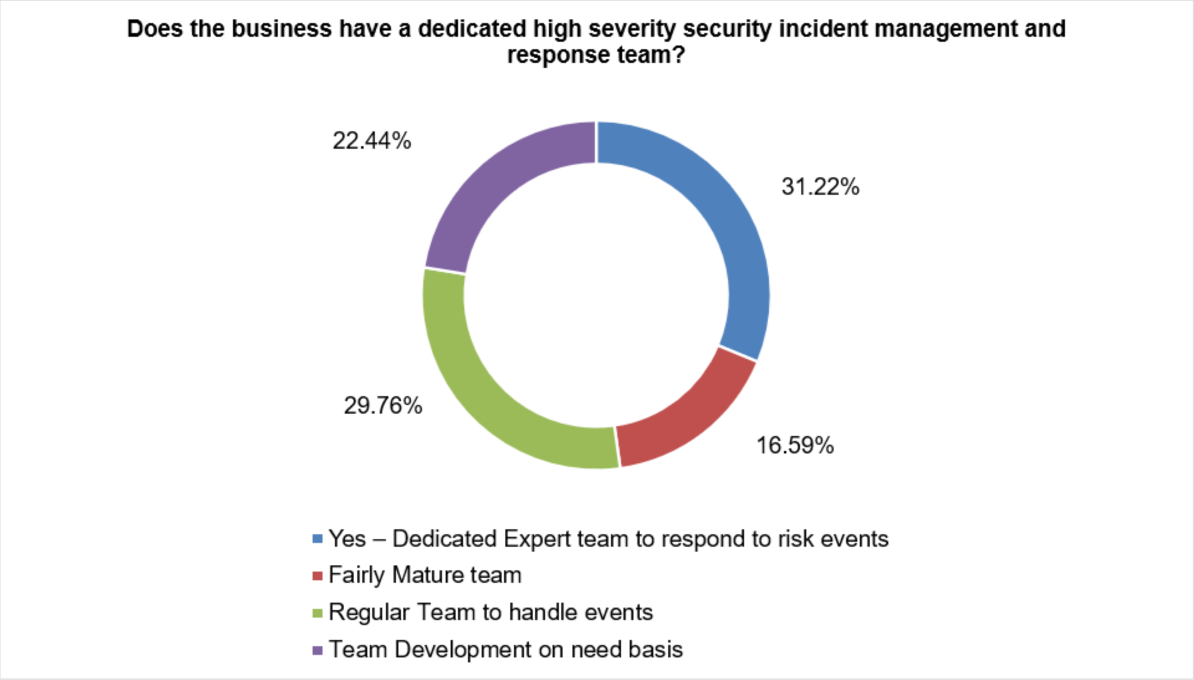


Figure 66

Table 76 shows that 63 of the total survey participants and Figure 67 shows that 25.85% of participants responded that 'Process in place only for few identified events' to action against suspicious behaviour in network security perimeter.

Table 76: Suspicious behaviour and IT infrastructure (cloud)

Is there any defined process to action against suspicious behaviour in network security perimeter? (User logging, Intrusion identification, account hijacking, password failures)		
User Behaviour Mapping Tools	**No. of Responses**	**No. of Responses as % of Total**
Yes – Advance tools, communication channel and action items in place	89	43.41%
Yes – Process in place only for few identified events	63	30.73%
No process in place and actions are need based	53	25.85%
Total	**205**	**100.00%**

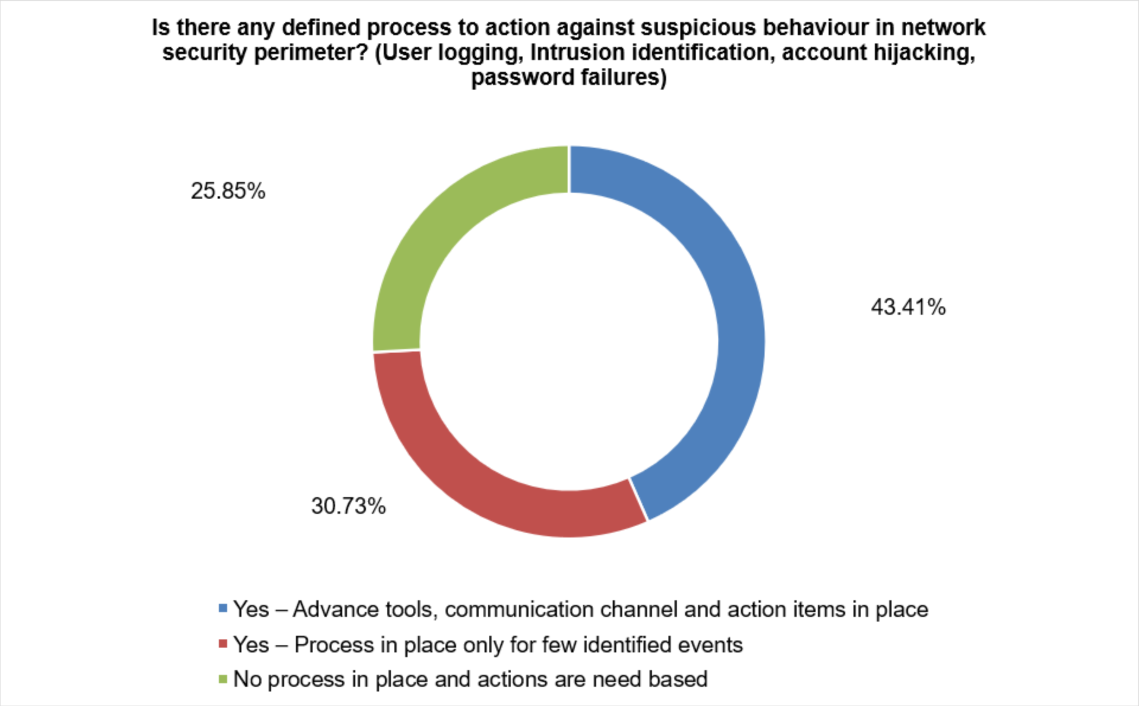


Figure 67

4.2.10 Reflection of research work concerning research question 2 (RQ2)

Need based emails & teleconferences (56.10%), incidents & problem meeting (56.10%), are found to be effective in managing cloud infrastructure related issues. Ongoing monitoring and alert mechanism (47.80%) help to link cloud architecture development, data integrity and IT security. IT infrastructure related changes involve both IT and non-IT resources of the organization (49.27%). Cloud architecture demand dedicated team (enterprise management / governance team is (36.10%)) with expertise to handle each area. Contractual obligations and global cloud management frameworks (40.49%) are required to control and operate on cloud. Need based policies and procedure (50.73%) to operate cloud help to evaluate cloud infrastructure effectives and business value delivery. Aligning cloud operations goals with organizational goals (45.37%) forms key theme to operate on cloud infrastructure. For IT security penetration testing is complex and involves number of teams (application-level control (48.29%), server level control (59.51%), network level control (52.68%), firewall rules (52.68%) and infrastructure elements. Server level security (59.51%) and control forms key to manage cloud infrastructure. Vulnerability assessment tools is helpful (40.49%) to evaluate data security related incidents. Independent and dedicated governance teams (51.71%) are required to manage cloud security. Education to employees (43.90%) and secure date transfer methods (37.56%) are enforcement points for data security management. Data categorization (71.22%) forms key requisite for data integrity management and reduce risk (63.90%) arising out of data leakages (data loss). Data security management tools (61.46%) are must to manage data over cloud. Training programs (60.49%) are must for organization staff and 3rd Party cloud infrastructure management staff. Cyber-security tools (40.98%) and firewall controls (40.98%) help to manage distributed denial of services attack. Findings of intrusion protection systems are not shared outside organization (64.39%). User logging and traffic management does not help (34.63%) to filter data packet level information. Majority of organization uses data retention tools (44.39%). Devices that are attacked and comprised are isolated (46.83%).

4.2.11 Prominent Theme Emerging for RQ2 from survey.

The prominent theme emerging from responses received for RQ2 and RQ1 & RQ 2 can be categorised in to following:

1. There is a need of dedicated incident and security team within an organization

2. There is a need of legal expertise to manage and operate cloud infrastructure

3. Security testing is complex and lengthy process.

4. Data management over cloud requires expertise and dedicated human and technological resources

4.2.12 Reflection on RQ 1& RQ2 combined

Most participants agree to have strategic plan to manage data privacy and system security. Project management office is aware and manages data security and system security as a part of ongoing project implementations. Data backup jobs help to protect data loss. Data security and system security have technological directions and technological adoption process in place. ITIL framework help manage data security and system security. IT risk management framework encompasses data and system security related aspects. Static and dynamic assessment tools help to assess quality of data. 3rd Party data centre management team help to protect physical cloud infrastructure. Legal team develops specific contracts to manage cloud architecture and cloud infrastructure. All data and system security related aspects are covered by service level agreements within ITIL framework. Service desk agents are trained to some extent to handle data and security related incidents. Managing cloud infrastructure from 3rd party service provider is very complex. Identity and access management tools form key to manage access within organization. Dedicated tools and human resources required to manage alerts and monitoring system of cloud infrastructure. 3rd Party cloud users are handled separately. 3rd party organization help to manage cloud user background. Sharing information with cyber security teams will help improve cloud security. Cloud computing has added risk to data and security of the system.

4.2.13 RQ 1 and RQ2 emerging theme

1. IT Risk management framework is key to manage data and system security risk

2. Monitoring and alert mechanism required to operate on cloud infrastructure

3. Cloud infrastructure has added risk to data privacy and system security

4.2.14 Discussion of research question 3 (RQ3)

Below table shows linking of RQ3 with 3 survey questions.

Table 77: Linking of RQ3 with 3 survey questions (cloud governance)

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
12	How are roles and responsibilities of cloud governance teams segregated?	RQ3	Cloud Governance
15	How often skills and expertise of cloud service provider and cloud support team is evaluated?	RQ3	Cloud Governance
13	Is IT security team informed about actions required to prevent data leakages?	RQ3	Cloud Security

Table 78: Linking of RQ1, RQ2 and RQ3 with 7 survey questions (cloud security)

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
28	Who governs and addresses the issue arising out of technological changes that poses threat to data and system security?	RQ1, RQ2, RQ3	Cloud Governance
30	Do you have dedicated budget and investment management framework to support Data and system security?	RQ1, RQ2, RQ3	Cloud Governance
39	As a part of business continuity plans, do you identify and reserve resources within team who deal with data and system security?	RQ1, RQ2, RQ3	Cloud Governance
42	How do you ensure the monitoring in everyday operations?	RQ1, RQ2, RQ3	Cloud Governance
40	Do you schedule employee and 3rd Party education programs for cloud security?	RQ1, RQ2, RQ3	Cloud Security
43	How do you ensure audit and compliance requirement for cloud security?	RQ1, RQ2, RQ3	Cloud Security
46	How do you monitor, measure, and maintain ethical controls within team to ensure culture of trust and responsibility within team?	RQ1, RQ2, RQ3	Cloud Security

The column “Question No.” in above table shows the sequence number in actual questionnaire emailed to participants.

Below shows the responses received for RQ3 from survey Participants:

Table 79 shows that 92 of the total survey participants and Figure 68 shows that 44.88% of participants responded that ‘Through Project Management, On-Going Monitoring and Alert Mechanism and Frequency Based Evaluation’ are method to segregate roles & responsibilities of IT Infrastructure (Cloud) governance team.

Table 79: Segregation of roles & responsibility of cloud governance teams

How are the roles and responsibilities of IT infrastructure (Cloud) governance teams segregated?		
Segregation of roles and responsibilities of IT infrastructure (Cloud) governance teams	**No. of Responses**	**No. of Responses as % of Total**
Through Project Management	54	26.34%
On-Going Monitoring and Alert Mechanism	71	34.63%
Frequency Based Evaluation	40	19.51%
Combination of All of these	92	44.88%
Total	**205**	**100.00%**

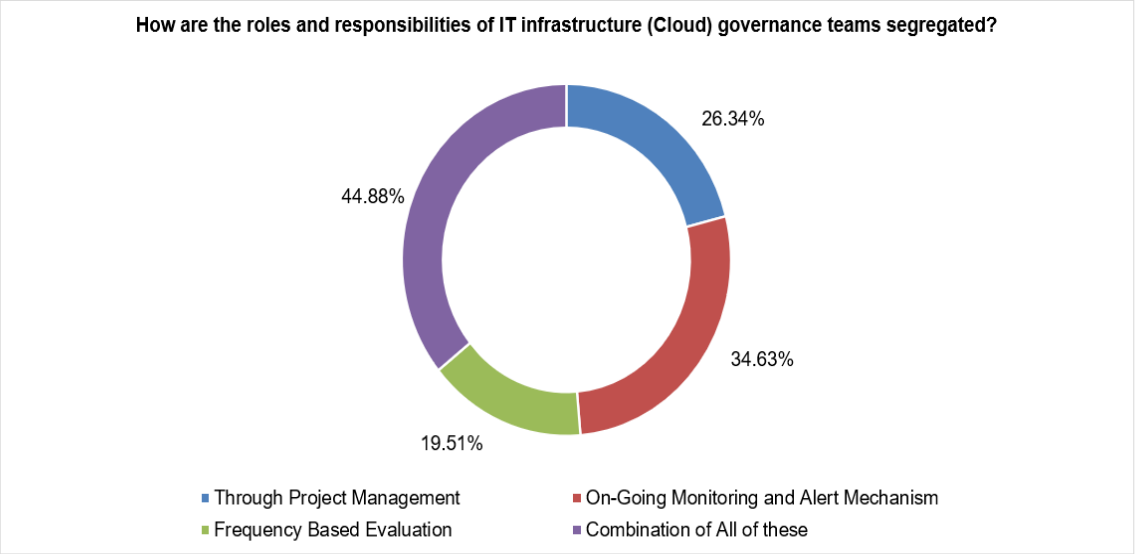


Figure 68

Table 80 shows that 83 of the total survey participants and Figure 69 shows that 40.49% of participants responded that ‘Quarterly’ assessment of skills and expertise of IT infrastructure (Cloud) service provider and the IT infrastructure (Cloud) support teams.

Table 80: Skills set of IT infrastructure support teams

How often are skills and expertise of your IT infrastructure (Cloud) service provider and the IT infrastructure (Cloud) support team evaluated?		
Skill set and expertise of IT support Teams	**No. of Responses**	**No. of Responses as % of Total**
Monthly	41	20.00%
Quarterly	83	40.49%
Half Yearly	29	14.15%
Annually	40	19.51%
Others (specify)	12	5.85%
Total	**205**	**100.00%**

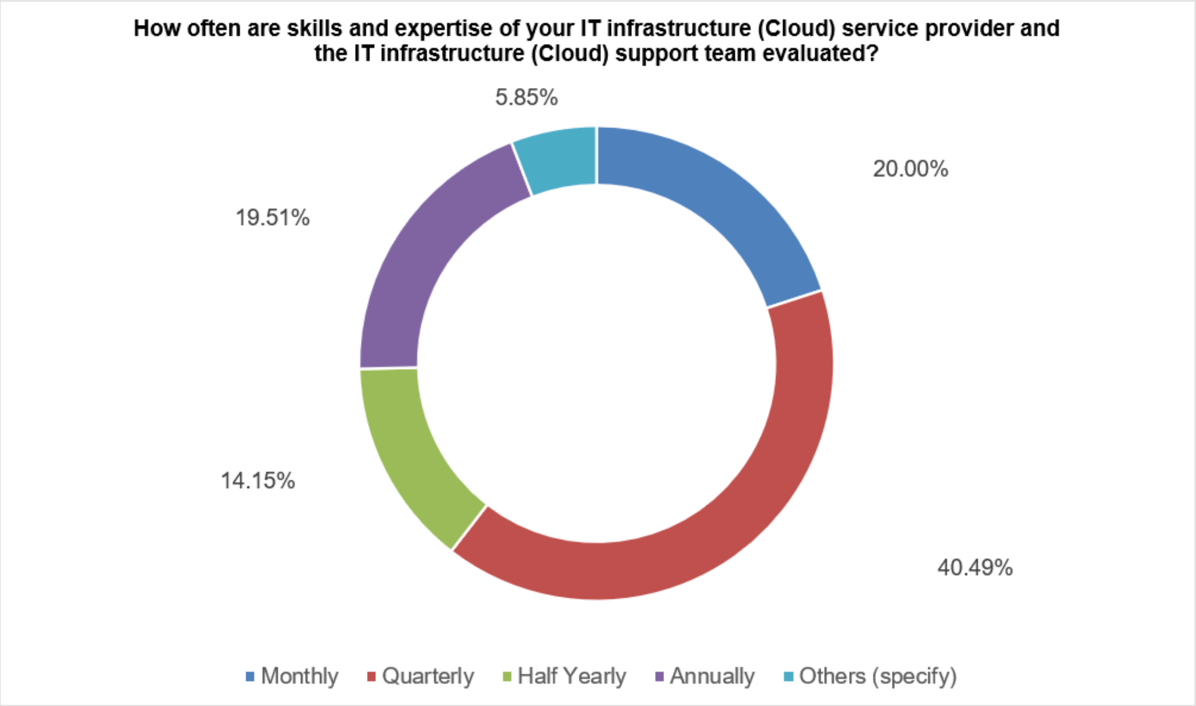


Figure 69

Table 81 shows that 146 of the total survey participants and Figure 70 shows that 40.49% of participants responded that IT security team / employees are informed about actions required to prevent data leakages.

Table 81: Education on data leakages to IT infrastructure support teams

Are the IT security team / employees informed about actions required to prevent data leakages?		
Information of Data Leakages	**No. of Responses**	**No. of Responses as % of Total**
Yes	146	71.22%
No	37	18.05%
Unsure	22	10.73%
Total	**205**	**100.00%**

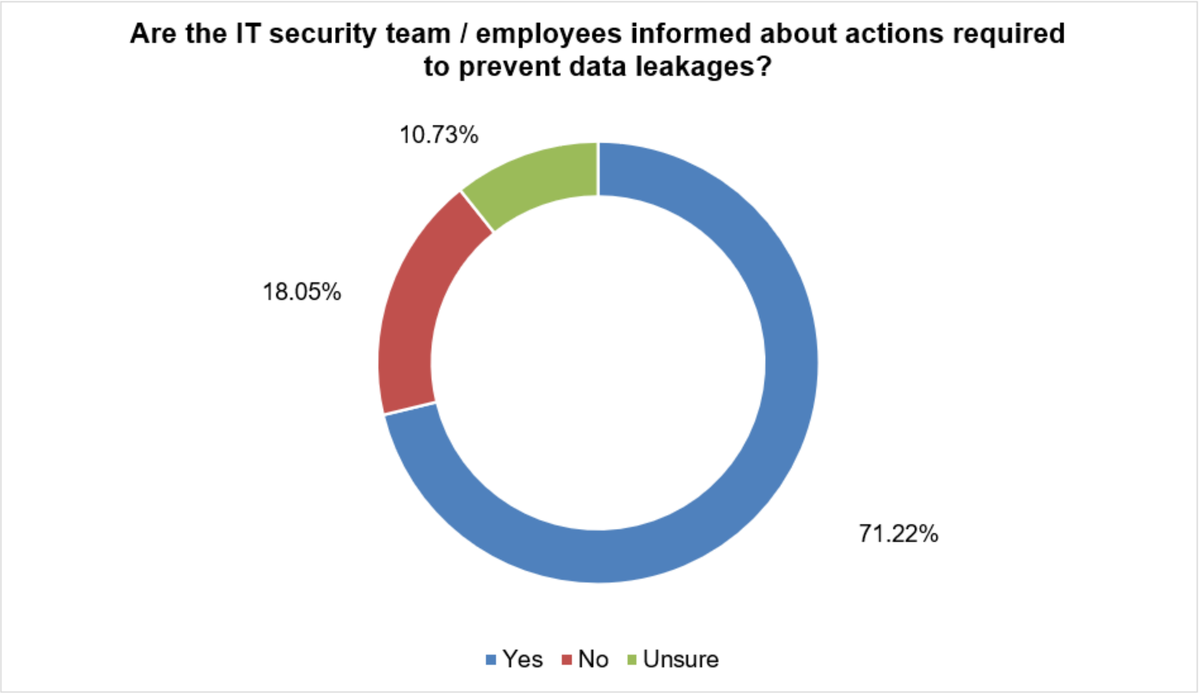


Figure 70

Below are survey responses for RQ1, RQ2 and RQ3:

Table 82 shows that 78 of the total survey participants and Figure 71 shows that 38.05% of participants responded that 'Dedicated IT infrastructure (Cloud) Architecture and IT security Team' are governing and addressing the issues that may arise out of technological changes which pose a threat to data and system security.

Table 82: Accountability and data & system security risk

Who governs and addresses the issues that may arise out of technological changes which pose a threat to data and system security?		
Accountability Teams	**No. of Responses**	**No. of Responses as % of Total**
Dedicated IT infrastructure (Cloud) Architecture and IT security Team	78	38.05%
IT Management / Governance Forum	67	32.68%
IT Risk Management Team	26	12.68%
Respective Technology Users	34	16.59%
Total	**205**	**100.00%**

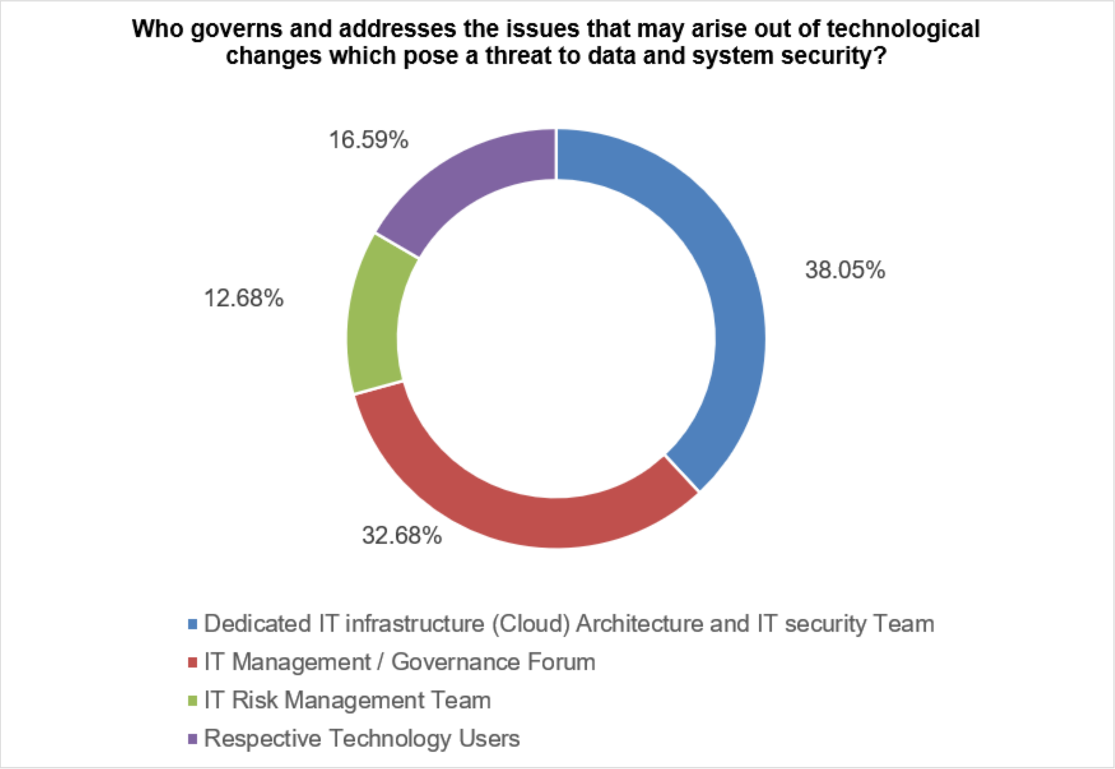


Figure 71

Table 83 shows that 88 of the total survey participants and Figure 72 shows that 38.05% of participants responded that “Annual financial investment and budget planning provides required support to manage data and system security for both projects and operational activities and sets asides considerable proportion of funds”.

Table 83: Financial commitment for data and system security

Does the business have a dedicated budget and investment management framework to support Data and system security?		
Budget Plan	**No. of Responses**	**No. of Responses as % of Total**
Yes – Annual financial investment and budget planning provides required support to manage data and system security for both projects and operational activities and sets asides considerable proportion of funds	88	42.93%
Yes – Annual budget planning considers the need of data and system security but does not set asides funds	54	26.34%
Yes – Annual budget planning considers the data and system security but does not set asides dedicated funds	23	11.22%
No – Annual budget planning does not provide support for data and system security needs and responsibilities around this are with a project development team to consider investment	40	19.51%
Total	**205**	**100.00%**

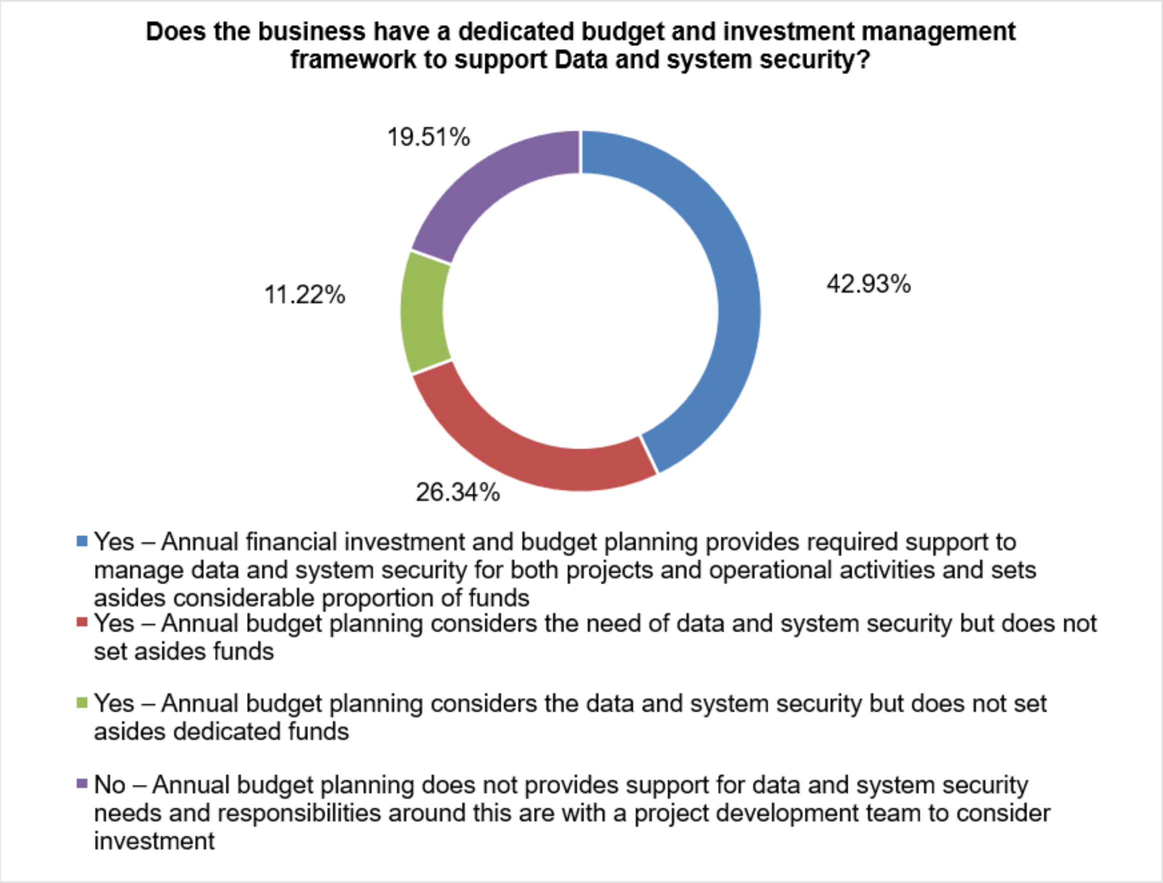

Does the business have a dedicated budget and investment management framework to support Data and system security?
19.51%
42.93%
11.22%
26.34%
🟦 Yes – Annual financial investment and budget planning provides required support to manage data and system security for both projects and operational activities and sets asides considerable proportion of funds
🟥 Yes – Annual budget planning considers the need of data and system security but does not set asides funds
🟩 Yes – Annual budget planning considers the data and system security but does not set asides dedicated funds
🟪 No – Annual budget planning does not provides support for data and system security needs and responsibilities around this are with a project development team to consider investment

Figure 72

Table 84 shows that 85 of the total survey participants and Figure 73 shows that 38.05% of participants responded that ‘Resources are identified based on skills and the ones dealing with Data and system security are identified separately to maintain business continuity plan’.

Table 84: Business continuity plan data and system security

As a part of business continuity plans, does the business identify and reserve resources within a team who deal with data and system security?		
Business Continuity plan	**No. of Responses**	**No. of Responses as % of Total**
Yes – Resources are identified based on skills and the ones dealing with Data and system security are identified separately to maintain business continuity plan	85	41.46%
Yes – Resources are identified based on skills; however no special emphasis is given for resources dealing with data and system security	54	26.34%
No – Resources are identified based on business-critical operations irrespective of their relation to data and system security	40	19.51%
No – Data and system security does not play parameter to plan business continuity plan with resources	26	12.68%
Total	**205**	**100.00%**

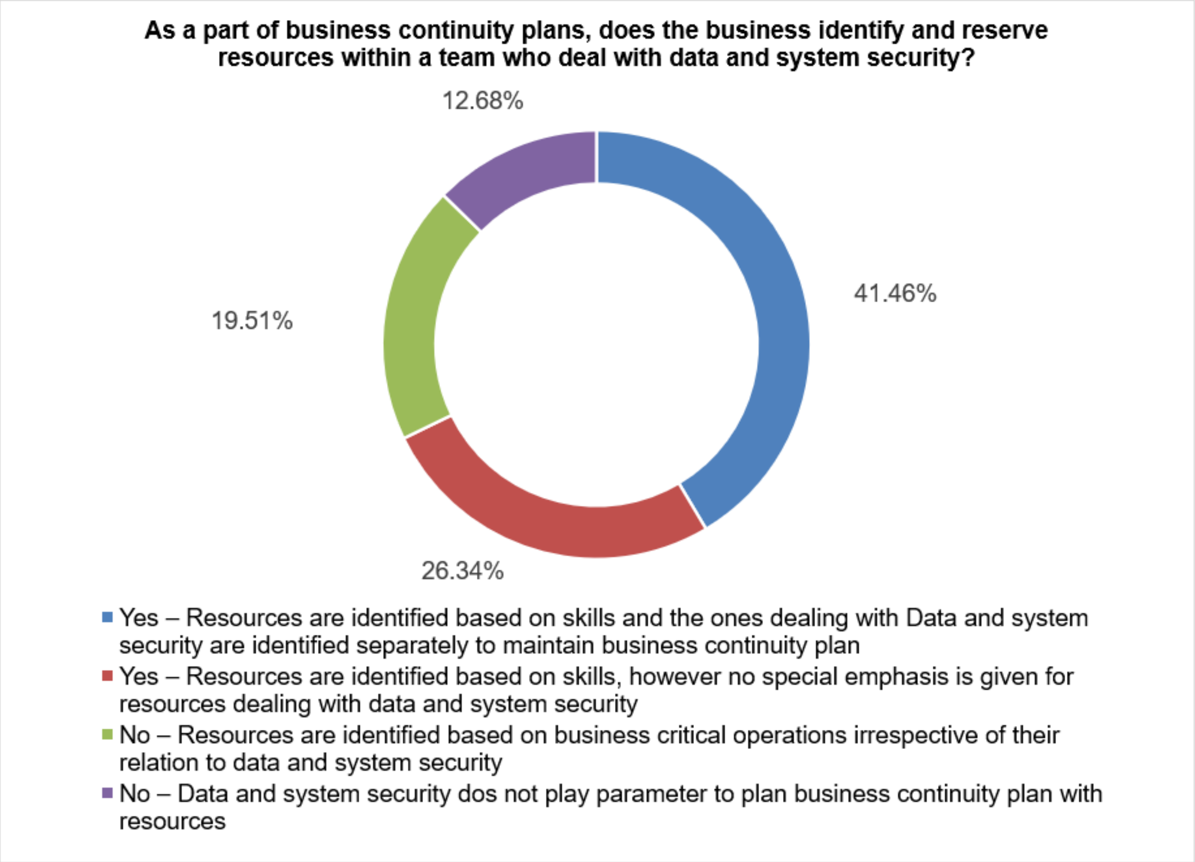

As a part of business continuity plans, does the business identify and reserve resources within a team who deal with data and system security?
12.68%
41.46%
19.51%
26.34%
🟦 Yes – Resources are identified based on skills and the ones dealing with Data and system security are identified separately to maintain business continuity plan
🟥 Yes – Resources are identified based on skills, however no special emphasis is given for resources dealing with data and system security
🟩 No – Resources are identified based on business critical operations irrespective of their relation to data and system security
🟪 No – Data and system security dos not play parameter to plan business continuity plan with resources

Figure 73

Table 85 shows that 78 of the total survey participants and Figure 74 shows that 38.05% of participants responded that 'Monitoring and logging is selective and enabled only for business-critical application performing financial transaction' while enabling monitoring in everyday operations.

Table 85: Monitoring of IT infrastructure (cloud)

How does the business enable monitoring in everyday operations?		
Monitoring Plan	**No. of Responses**	**No. of Responses as % of Total**
Monitoring, logging information collections and storage of Applications, processes, Hardware devices and user activities are enabled through automation scripts	71	34.63%
Monitoring and logging is selective and enabled only for business critical application performing financial transaction	78	38.05%
Monitoring and logging is enabled only for security tools	40	19.51%
Monitoring and logging information is not available for any application or processes	16	7.80%
Total	**205**	**100.00%**

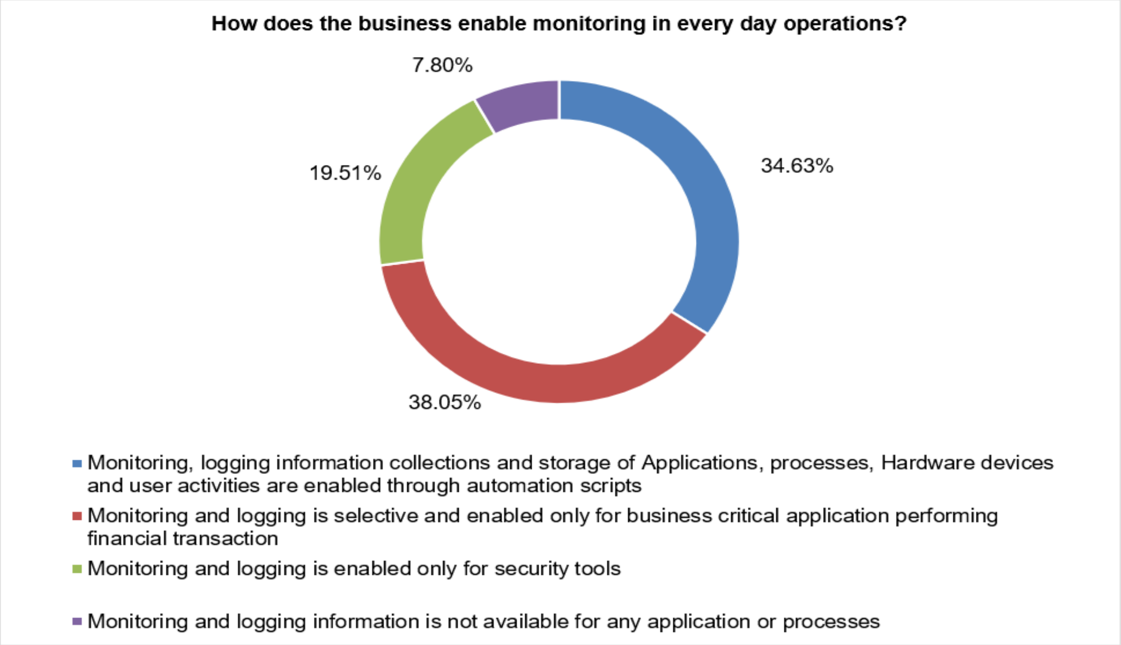


Figure 74

Table 86 shows that 70 of the total survey participants and Figure 75 shows that 34.15% of participants responded that ‘Frequent training program based on need are conducted for identified users’ while employing 3rd party education programs.

Table 86: 3rd party education on data & system security

Does the business schedule employ 3rd Party education programs for IT Infrastructure (Cloud) security?		
3rd Party Education Plan	**No. of Responses**	**No. of Responses as % of Total**
Yes – Regular training and development program are conducted	62	30.24%
Yes – Frequent training program based on need are conducted for identified users	70	34.15%
No – There no such need	58	28.29%
Human resources are responsible to educate employee and system users	15	7.32%
Total	**205**	**100.00%**

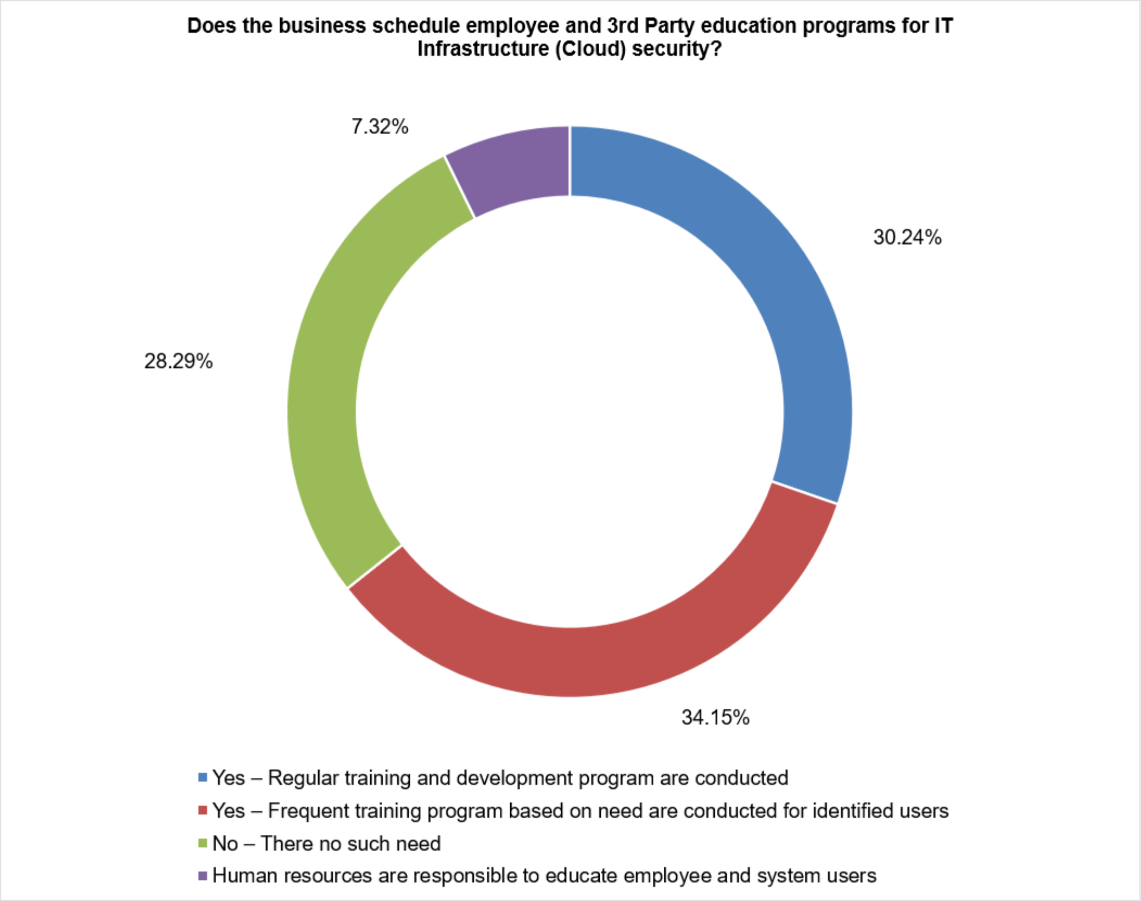


Figure 75

Table 87 shows that 78 of the total survey participants and Figure 76 shows that 38.05% of participants responded that ‘Need based involvement of team members to handle audit and compliance incidents’ to ensure audit and compliance requirement for IT Infrastructure (Cloud) security.

Table 87: Audit and compliance for cloud security

How does the business ensure audit and compliance requirement for IT Infrastructure (Cloud) security?		
Audit and Compliance	**No. of Responses**	**No. of Responses as % of Total**
Dedicated team to support audit and compliance requirements on regular basis	64	31.22%
Need based involvement of team members to handle audit and compliance incidents	78	38.05%
Only Annual review and mitigation of Audit and compliance issues	38	18.54%
No Audit and compliance framework	25	12.20%
Total	**205**	**100.00%**

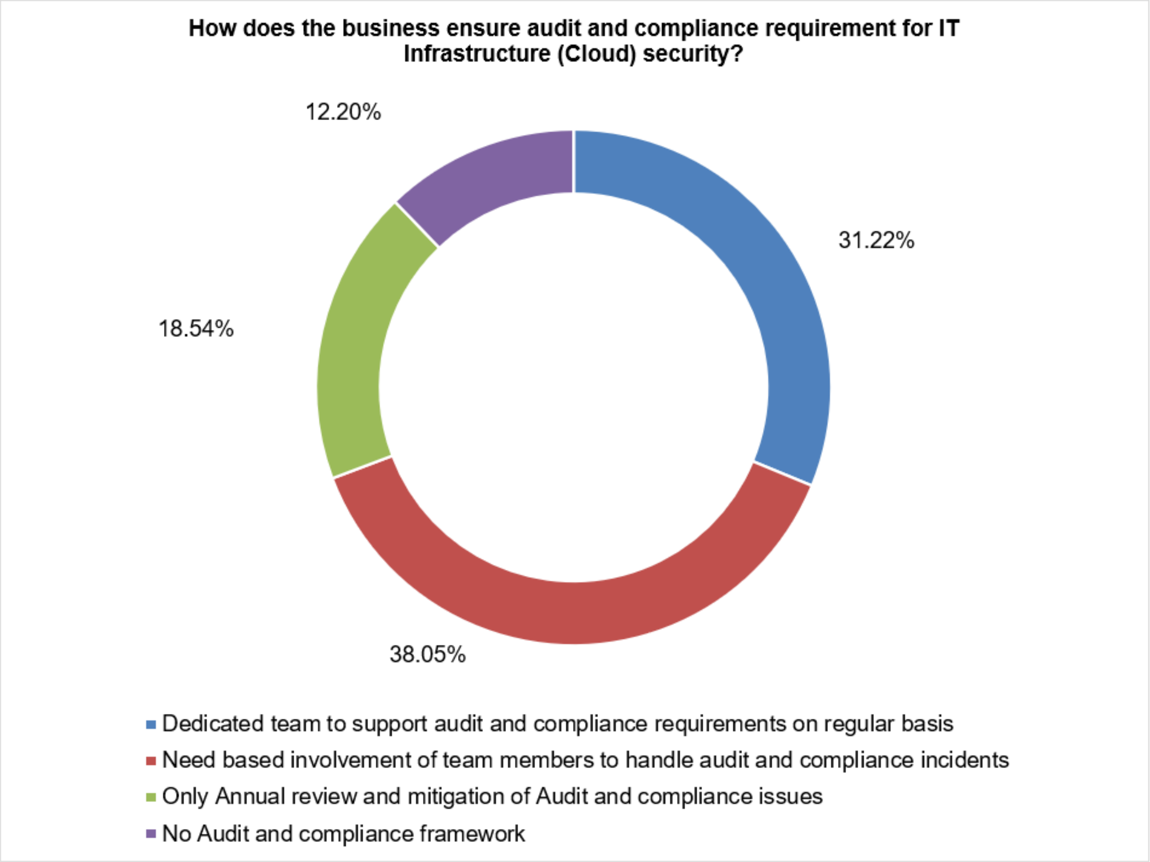


Figure 76

Table 88 shows that 87 of the total survey participants and Figure 77 shows that 42.44% of participants responded that 'Regular Team building exercise and awareness about responsibility towards organization is educated to all team members' to measure and maintain ethical controls within team to ensure culture of trust and responsibility within team.

Table 88: Ethical Controls for Team & Culture Development

Does the business measure and maintain ethical controls within team to ensure culture of trust and responsibility within team?		
Team Development Plan	**No. of Responses**	**No. of Responses as % of Total**
Regular Team building exercise and awareness about responsibility towards organization is educated to all team members	87	42.44%
Occasional meeting within team help to develop team and culture	74	36.10%
Human resources handle this exercise as per organization culture	28	13.66%
There is no such activity planned	50	24.39%
Total	**205**	**100.00%**

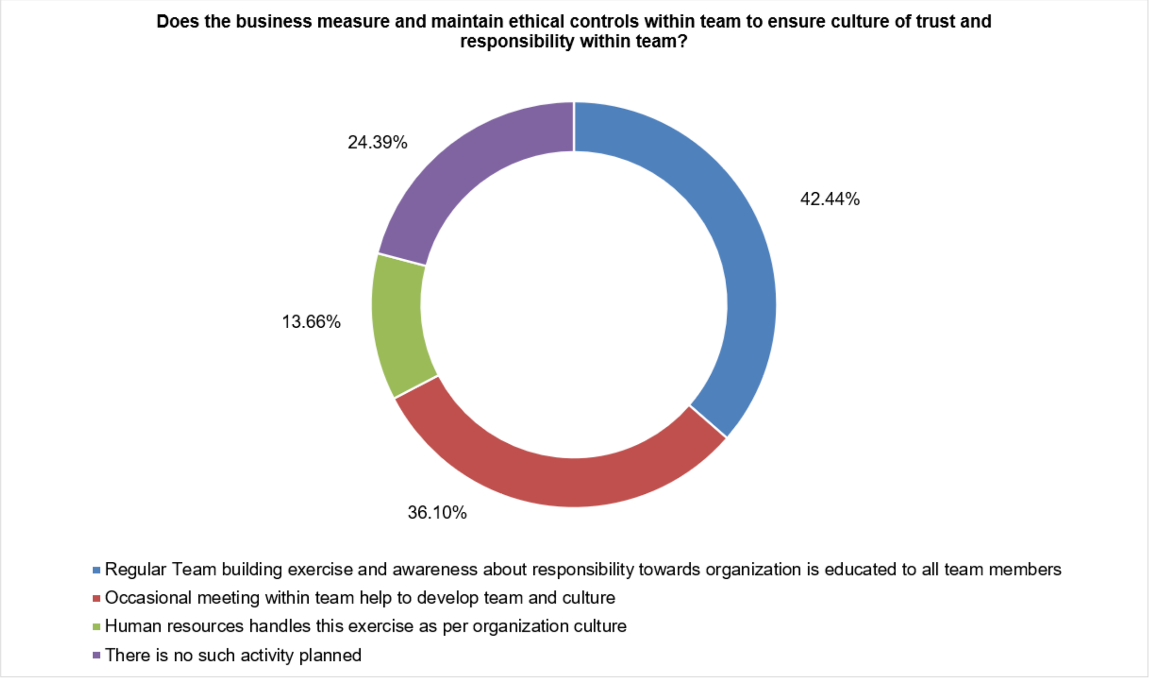


Figure 77

4.2.15 Reflection of research work concerning research question 3 (RQ3)

Roles and responsibilities of cloud infrastructure support teams are managed through alert and monitoring during day-to-day operations (through combination (44.88%) of project, engagement (26.34%), on-going monitoring and alert mechanism (34.63%), frequency-based evaluation (19.51%)). Majority of the organizations (40.49%) assess roles and responsibility of cloud infrastructure support team quarterly. IT security teams are informed (71.22%) regularly to prevent data leakages.

4.2.16 Prominent theme emerging for research question 3 (RQ3) from survey feedback

The prominent theme emerging from responses received for RQ3 can be categorised in to following:

1. Review of roles and responsibility is required for IT security team

2. Dedicated budget is required to manage cloud governance framework

3. Business continuity plans needs dedicated resources to handle data and system security

4. Ethical controls forms key to train resources to manage cloud infrastructure

4.2.17 Prominent theme emerging for research question RQ1, RQ2 and RQ3

Dedicated team handle change in cloud architecture and risks arising out of it. Annual budget is allocated to manage cloud infrastructure. Business continuity plan manage dedicated resources to manage data privacy and system security. Cloud audit involves need based engagement with cloud infrastructure management resources. Team building exercise to develop ethical control within organization.

4.2.18 Discussion of Research Question 4 (RQ4)

Below table shows linking of RQ4 with 18 survey questions.

Table 89: linking of RQ4 with 3 survey questions.

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
9	What are governance structure for Cloud due to digital transformation?	RQ4	Cloud Governance
7	Are vulnerability assessment tools sufficient to report data security related incidents through digital platforms?	RQ4	Cloud Security
14	Has digital transformation added new data leakages areas?	RQ4	Cloud Security

Table 90: linking of RQ4 with RQ1, RQ2 and RQ4 survey questions.

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
24	What is the frequency to update Security Certificates (SSL)?	RQ1, RQ2, RQ4	Cloud Security
25	What is the frequency to upgrade monitoring and alert mechanism?	RQ1, RQ2, RQ4	Cloud Security
29	Do you monitor and log user activities?	RQ1, RQ2, RQ4	Cloud Security
37	Is there any defined process to handle 3rd Party System Users?	RQ1, RQ2, RQ4	Cloud Security
38	Have you defined key risk parameters for cloud infrastructure resources?	RQ1, RQ2, RQ4	Cloud Security
39	Is there a job rotation within IT security team?	RQ1, RQ2, RQ4	Cloud Security

Table 91: linking of RQ4 with RQ1, RQ2, RQ3 and RQ4 survey questions.

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
34	What are steps to manage and control the risk related events identified for data and system security? (RQ1, RQ2, RQ3, RQ4)	RQ1, RQ2, RQ3, RQ4	Cloud Governance
37	How do you keep control over emergency changes to mitigate risk of system downtime and resolve high impact incidents? (RQ1, RQ2, RQ3, RQ4)	RQ1, RQ2, RQ3, RQ4	Cloud Governance
40	Does your IT Security plan include data and system security specific controls?	RQ1, RQ2, RQ3, RQ4	Cloud Governance
27	Do you have Risk event and risk mitigation plan in case of cyber-attack or threat detection cases?	RQ1, RQ2, RQ3, RQ4	Cloud Security
30	Do you plan OR have you implemented machine learning and Artificial intelligence to respond to suspicious activities by internal or external users?	RQ1, RQ2, RQ3, RQ4	Cloud Security
45	How do you monitor and govern test environments and production environments over cloud infrastructure?	RQ1, RQ2, RQ3, RQ4	Cloud Security

Table 92: linking of RQ4 with RQ2 and RQ4 survey questions.

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
19	What Bank specific parameters are considered while configuring data leakage prevention tools?	RQ2, RQ4	Cloud Security
22	Does traffic monitoring tool help monitor users from all channels?	RQ2, RQ4	Cloud Security

The column "Question No." in above table shows the sequence number in actual questionnaire emailed to participants.

Below shows the responses received for RQ4 from survey Participants:

Table 93 shows that 116 of the total survey participants and Figure 78 shows that 56.59% of participants responded that ‘New IT infrastructure (Cloud) Monitoring Indicators’ are used to manage / govern IT infrastructure (Cloud) related to digital transformation.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 93: Management / governance structures for IT infrastructure (cloud) related to digital transformation.

What are the management / governance structures for IT infrastructure (Cloud), related to digital transformation?		
Management / governance structures	**No. of Responses**	**No. of Responses as % of Total**
Addition of New stakeholders	63	30.73%
Development of New IT infrastructure (Cloud) performance Parameters	109	53.17%
New IT infrastructure (Cloud) Monitoring Indicators	116	56.59%
Development of New IT infrastructure (Cloud) services to meet digital Platform requirements	103	50.24%
Others: type / write details	3	1.46%
Total	**205**	**100.00%**

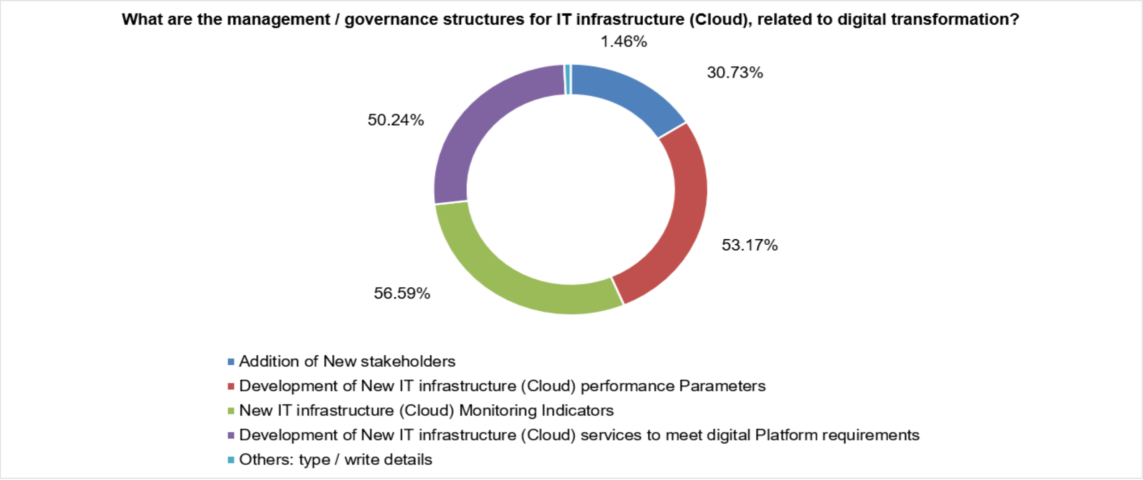


Figure 78

Table 94 shows that 83 of the total survey participants and Figure 79 shows that 40.49% of participants responded that vulnerability assessment tools are sufficient to report data security related incidents.

Table 94: Vulnerability assessment tools for IT infrastructure (cloud)

Are vulnerability assessment tools sufficient to report data security related incidents?		
Vulnerability assessment tools	**No. of Responses**	**No. of Responses as % of Total**
Yes	83	40.49%
No	60	29.27%
Unsure / don't know	62	30.24%
Total	**205**	**100.00%**

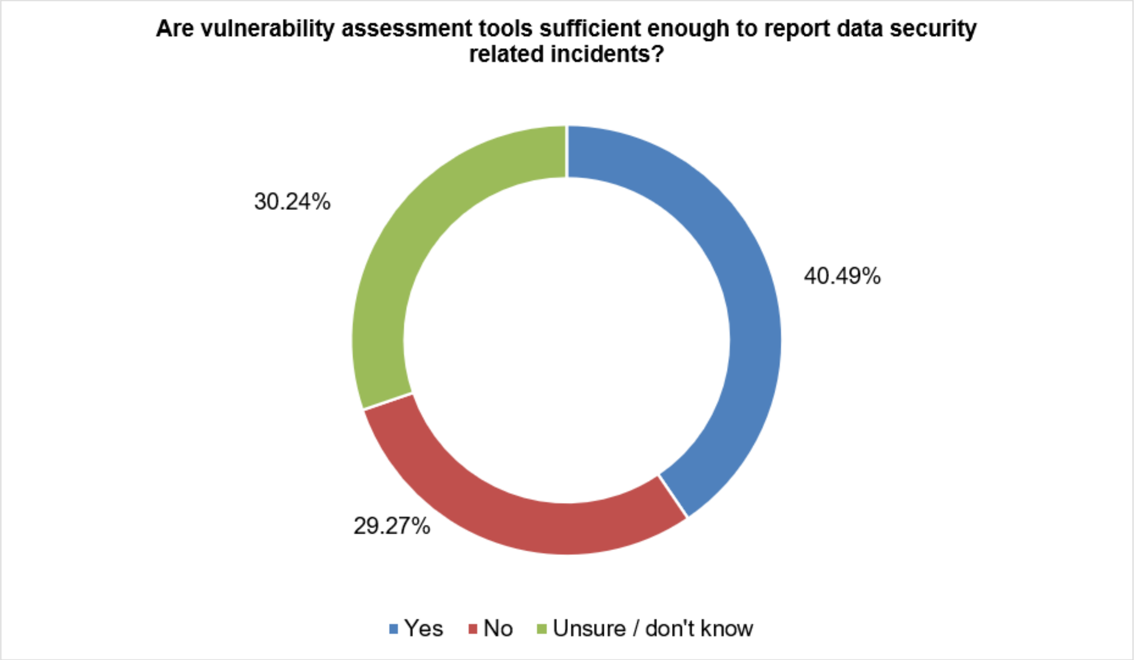


Figure 79

Table 95 shows that 93 of the total survey participants and Figure 80 shows that 45.37% of participants responded that digital transformation has added new data leakages areas.

Table 95: Digital transformation and data leakages

Has digital transformation added new data leakages areas?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Yes	93	45.37%
No	63	30.73%
Unsure	49	23.90%
Total	**205**	**100.00%**

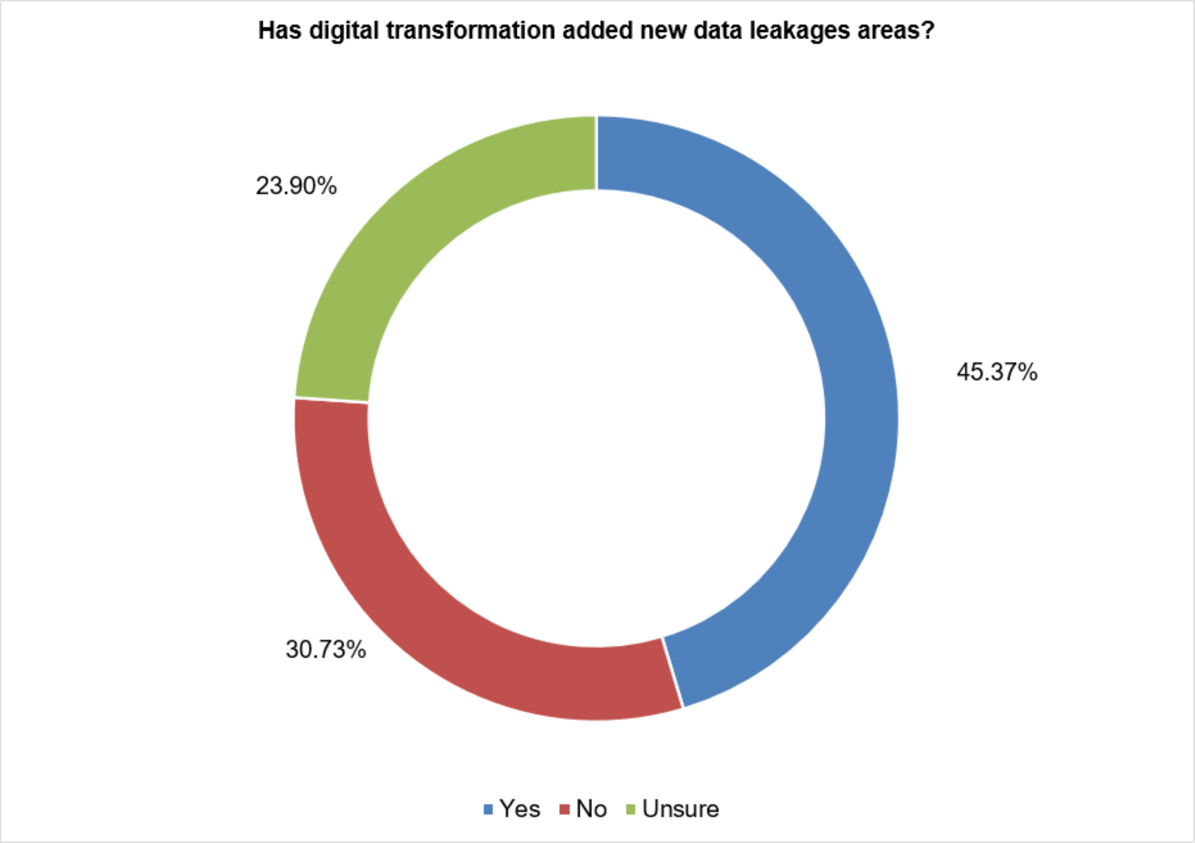


Figure 80

Table 96 shows that 75 of the total survey participants and Figure 81 shows that 36.59% of participants responded that ‘There is shared responsibility between IT risk and IT process management to respond to risk event’ to manage and control risk related events identified for data and system security.

Table 96: Risk event and controls for data & system security

What steps are in place to manage and control risk related events identified for data and system security?		
Control Mechanism	**No. of Responses**	**No. of Responses as % of Total**
There is a dedicated IT Risk and Incident management team that assess and responds to high severity risk events reported or identified by system users	59	28.78%
There is shared responsibility between IT risk and IT process management to respond to risk event	75	36.59%
There is a General IT incident management team contacted via helpdesk to inform and act on risk events	44	21.46%
There is no risk definition and impact is assessed based on incident reported	27	13.17%
Total	**205**	**100.00%**

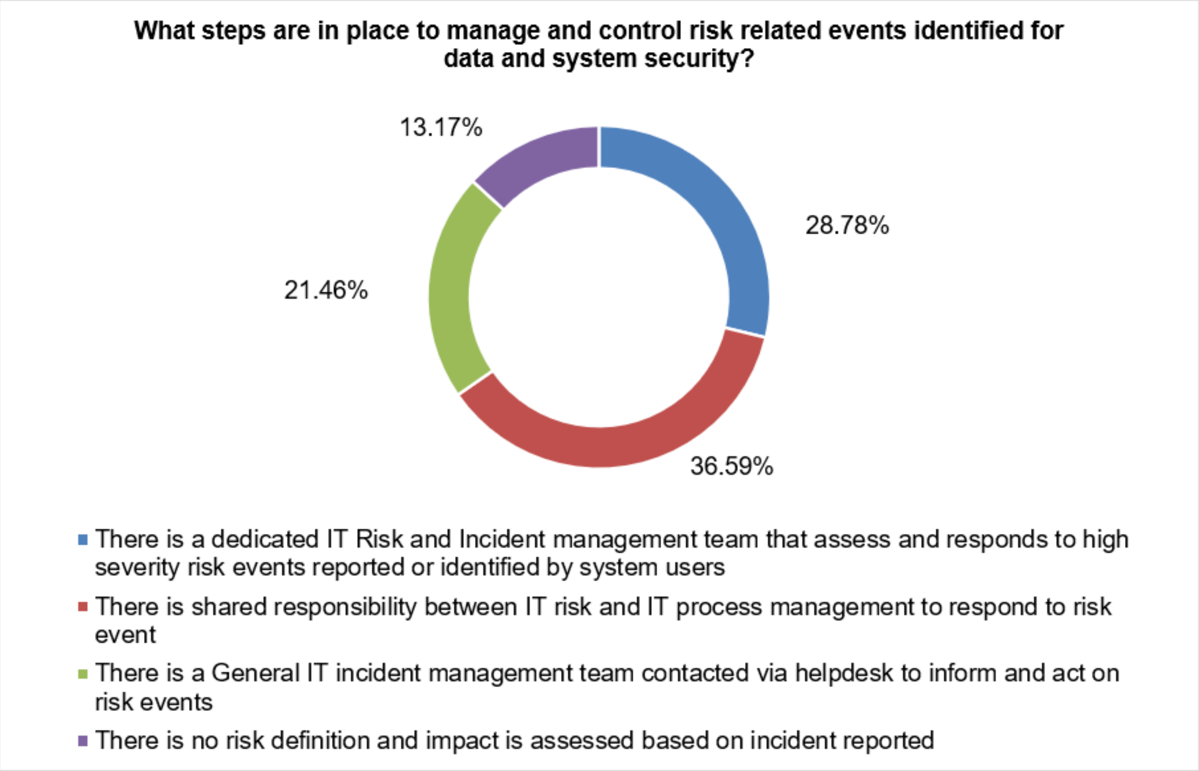

What steps are in place to manage and control risk related events identified for data and system security?
13.17%
28.78%
21.46%
36.59%
🟦 There is a dedicated IT Risk and Incident management team that assess and responds to high severity risk events reported or identified by system users
🟥 There is shared responsibility between IT risk and IT process management to respond to risk event
🟩 There is a General IT incident management team contacted via helpdesk to inform and act on risk events
🟪 There is no risk definition and impact is assessed based on incident reported

Figure 81

Table 97 shows that 75 of the total survey participants and Figure 82 shows that 36.59% of participants responded that ‘Emergency changes must be approved by governance forum from both company and 3rd part contractors. There is dedicated team to work on emergency changes to avoid failures’ and this keeps control over emergency changes to mitigate risk of system downtime and resolve high impact incidents.

Table 97: Emergency system changes and control over IT infrastructure

How does the business keep control over emergency changes to mitigate risk of system downtime and resolve high impact incidents?		
Emergency Change Control Mechanism	**No. of Responses**	**No. of Responses as % of Total**
Emergency changes must be approved by governance forum from both company and 3rd part contractors. There is dedicated team to work on emergency changes to avoid failures	94	45.85%
Emergency changes are responsibility of 3rd party contractors and IT service providers with no control from the company	52	25.37%
Emergency changes are treated as normal / standard changes and only need communication to relevant stakeholders and impacted parties (users)	59	28.78%
Total	**205**	**100.00%**

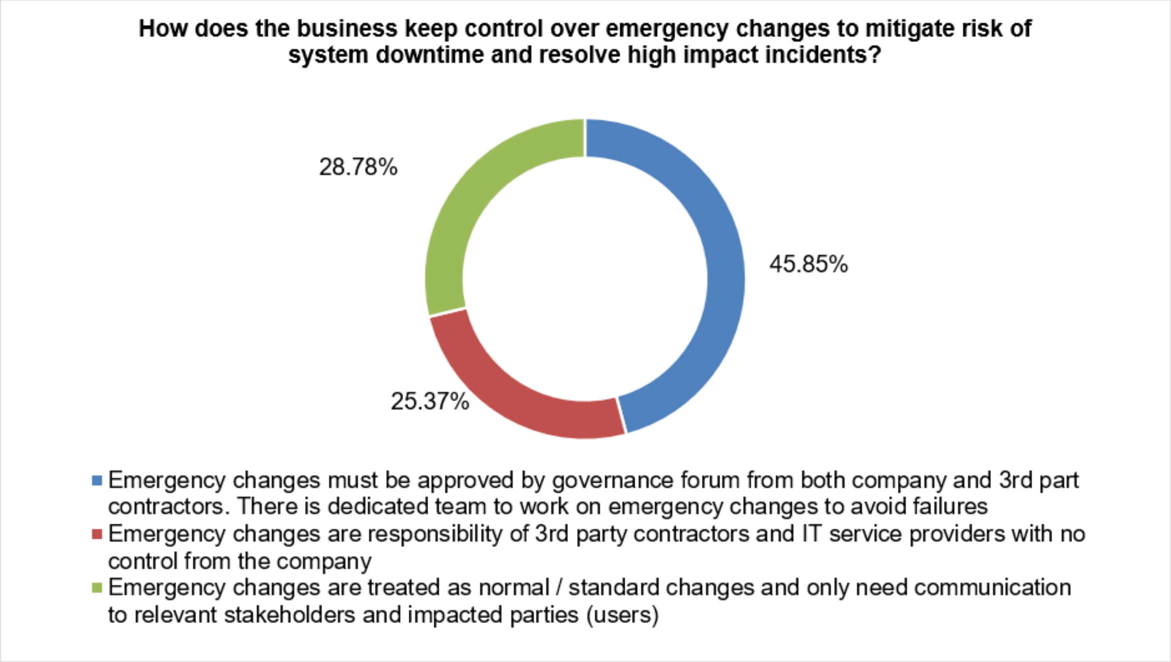


Figure 82

Table 98 shows that 77 of the total survey participants and Figure 83 shows that 37.07% of participants responded that ‘IT Security plan defines, implements, monitors and controls data and system security’ and helps data & security specific controls.

Table 98: IT security plan and data & system security specific controls

Does the IT Security plan include data and system security specific controls?		
IT Security plan	**No. of Responses**	**No. of Responses as % of Total**
Yes – IT Security plan defines, implements, monitors and controls data and system security	76	37.07%
Yes – IT Security Plan implements policies and procedures for data and system security	68	33.17%
Yes – IT security plan has provided guidelines and works on need basis to control data and system security	59	28.78%
No – IT Security plan is general methods to secure data and systems and does not categorise impact and risk to data and security	36	17.56%
Unsure / Don't know	21	10.24%
Total	**205**	**100.00%**

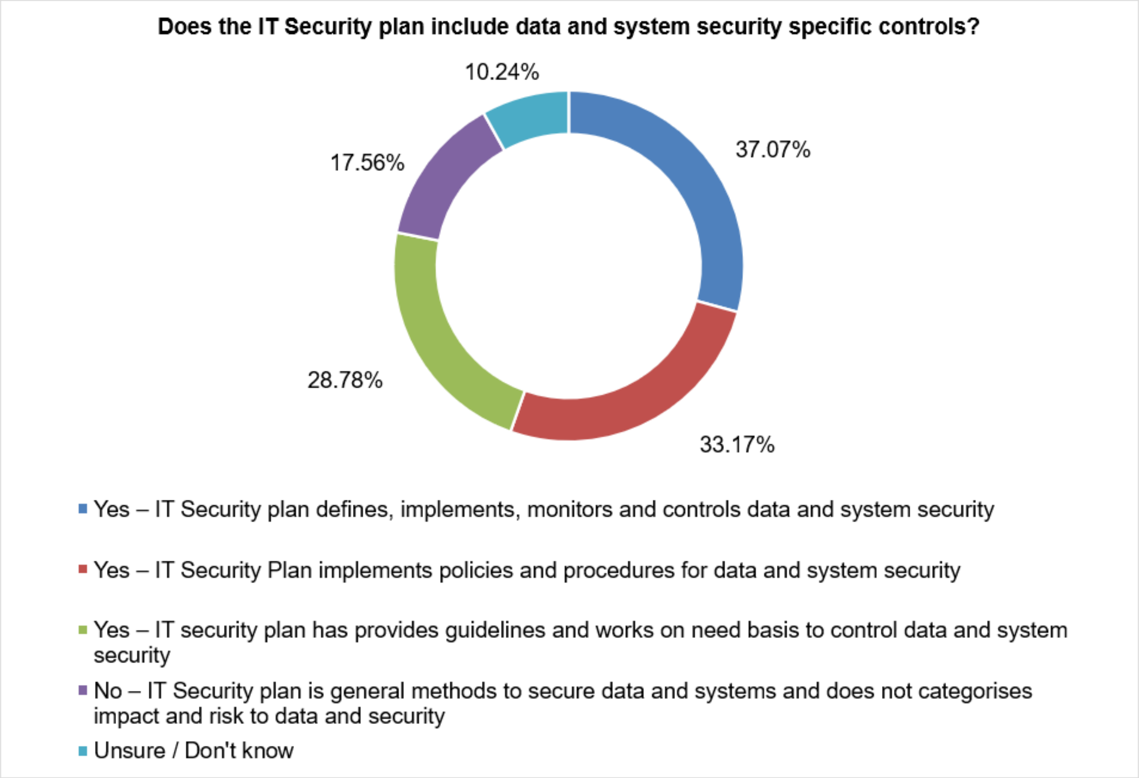


Figure 83

Table 99 shows that 91 of the total survey participants and Figure 84 shows that 37.07% of participants responded that ‘Account Information’ is most important parameter considered while configuring data leakage prevention tools. Individual information parameter control is 2nd most important parameter while configuring data leakage prevention tools.

(Survey Participants have selected more than one option while replying to this survey question. Total responses received for this survey question is 205)

Table 99: Company specific parameters for data leakage prevention

What company specific parameters are considered while configuring data leakage prevention tools?		
Company specific parameters for data leakage prevention	**No. of Responses**	**No. of Responses as % of Total**
All Parameter covering Individual Privacy Act	85	41.46%
Account Information	91	44.39%
Car Information	24	11.71%
Data collected from Digital Platforms	64	31.22%
All of these	71	34.63%

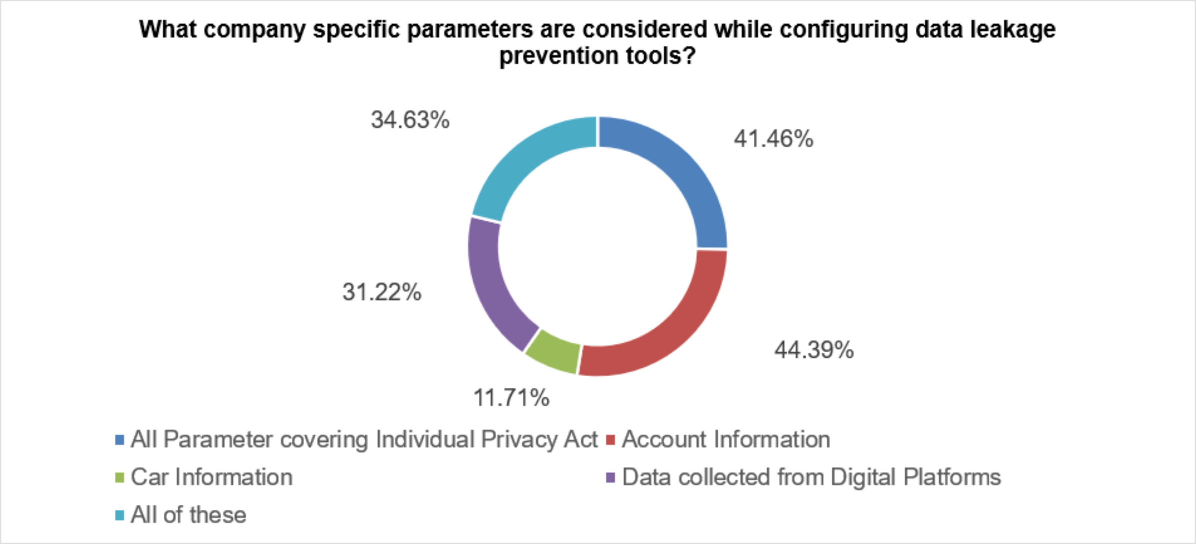


Figure 84

Table 100 shows that 77 of the total survey participants and Figure 85 shows that 37.56% of participants responded that traffic monitoring tools help monitor users from all channels.

Table 100: Traffic monitoring tools to monitor users.

Do traffic monitoring tools help monitor users from all channels?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Yes	77	37.56%
No	24	11.71%
Only to monitor traffic Load	36	17.56%
Separate Tool for content monitoring	28	13.66%
Unsure	40	19.51%
Total	**205**	**100.00%**

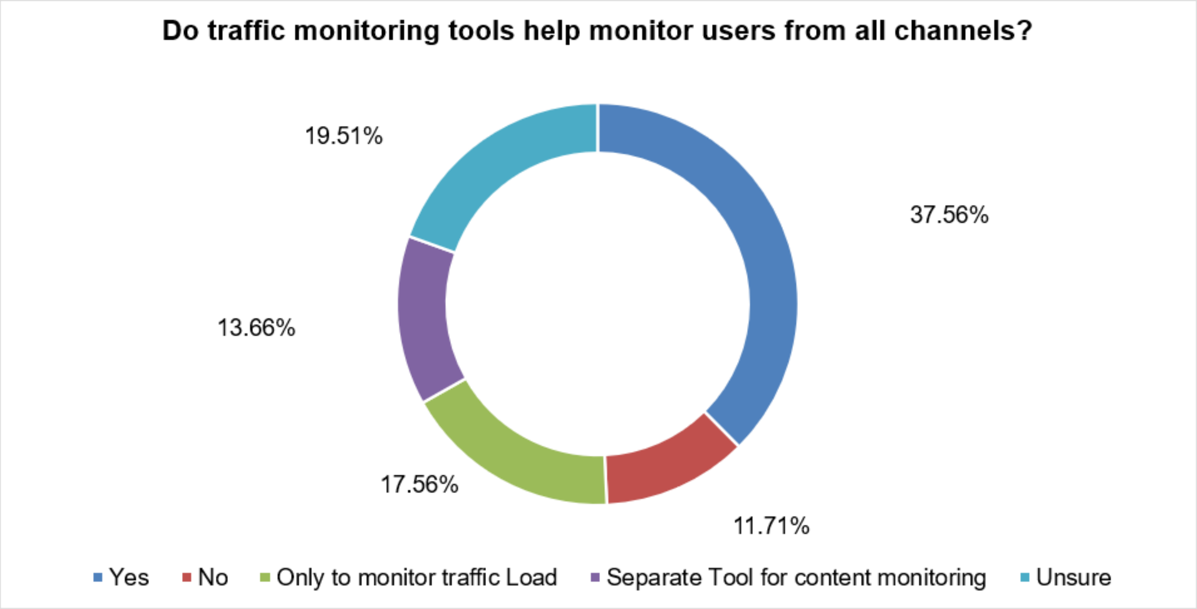


Figure 85

Table 101 shows that 64 of the total survey participants and Figure 86 shows that 37.56% of participants responded that Security Certificates (SSL) are updated ‘Quarterly’.

Table 101: Security certificate renewal for IT infrastructure (cloud)

How frequently are Security Certificates (SSL) updated?		
Frequency	**No. of Responses**	**No. of Responses as % of Total**
Monthly	33	16.10%
Quarterly	50	24.39%
Half Yearly	28	13.66%
Need Based / Vendor prescribed	64	31.22%
Unsure	30	14.63%
Total	**205**	**100.00%**

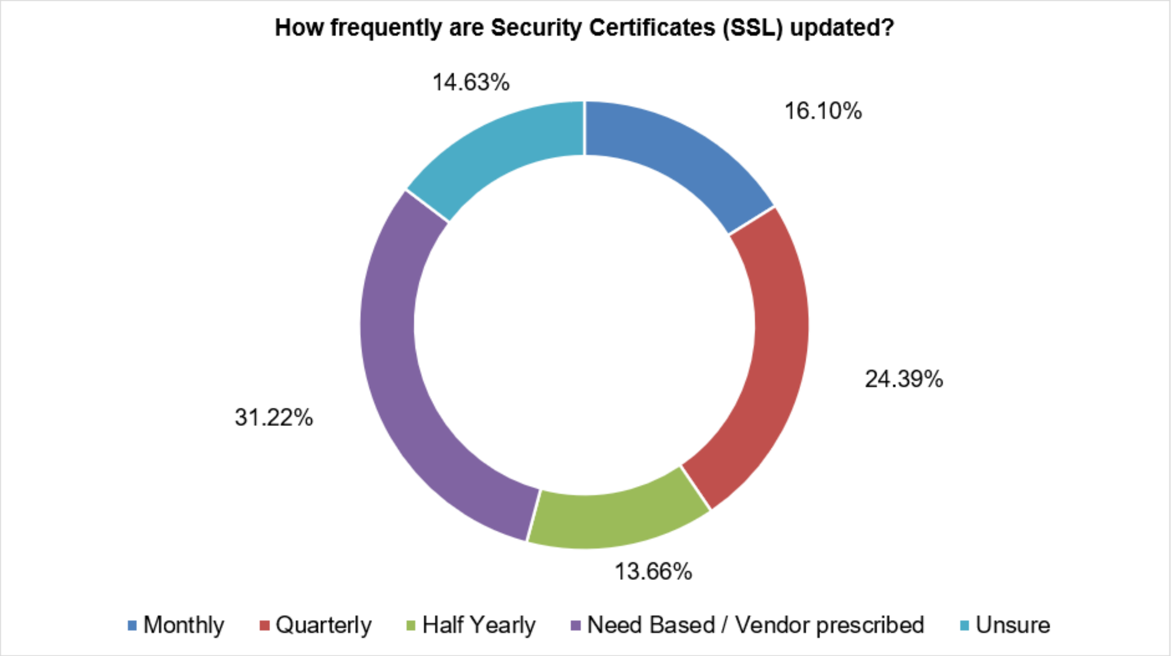


Figure 86

Table 102 shows that 69 of the total survey participants and Figure 87 shows that 37.56% of participants responded that ‘Need Based / Vendor prescribed’ upgrades to monitoring and alert mechanisms implemented for Security certificate renewal for IT infrastructure (cloud)

Table 102: Security certificate renewal for IT infrastructure (cloud)

How frequently are upgrades to monitoring and alert mechanisms implemented?		
Frequency	**No. of Responses**	**No. of Responses as % of Total**
Monthly	40	19.51%
Quarterly	56	27.32%
Half Yearly	16	7.80%
Need Based / Vendor prescribed	69	33.66%
Unsure	24	11.71%
Total	**205**	**100.00%**

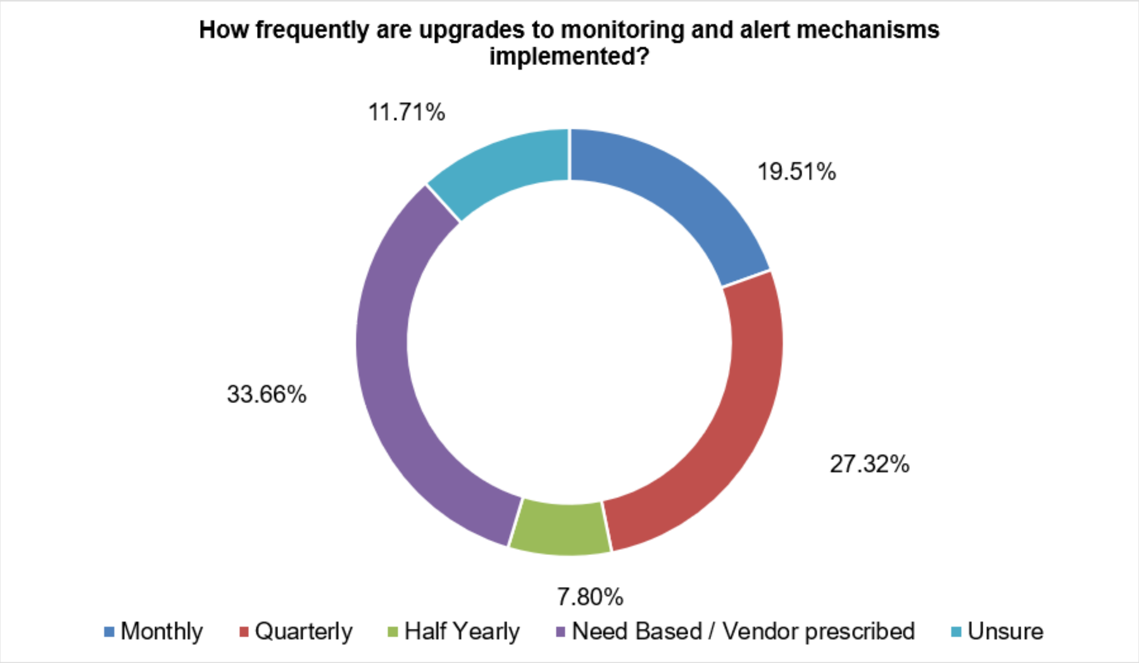


Figure 87

Table 103 shows that 82 of the total survey participants and Figure 88 shows that 37.56% of participants responded that business have a risk event and risk mitigation plan in case of cyber-attack or threat detection cases.

Table 103: Risk evens and risk mitigation plan for cyber-attacks on IT infrastructure

Does the business have a risk event and risk mitigation plan in case of cyber-attack or threat detection cases?		
Risk Events & Mitigation Plan	**No. of Responses**	**No. of Responses as % of Total**
Yes – Detailed Plan	82	40.00%
No Plan	48	23.41%
Tentative Plan for known events	50	24.39%
Development Under progress	25	12.20%
Total	**205**	**100.00%**

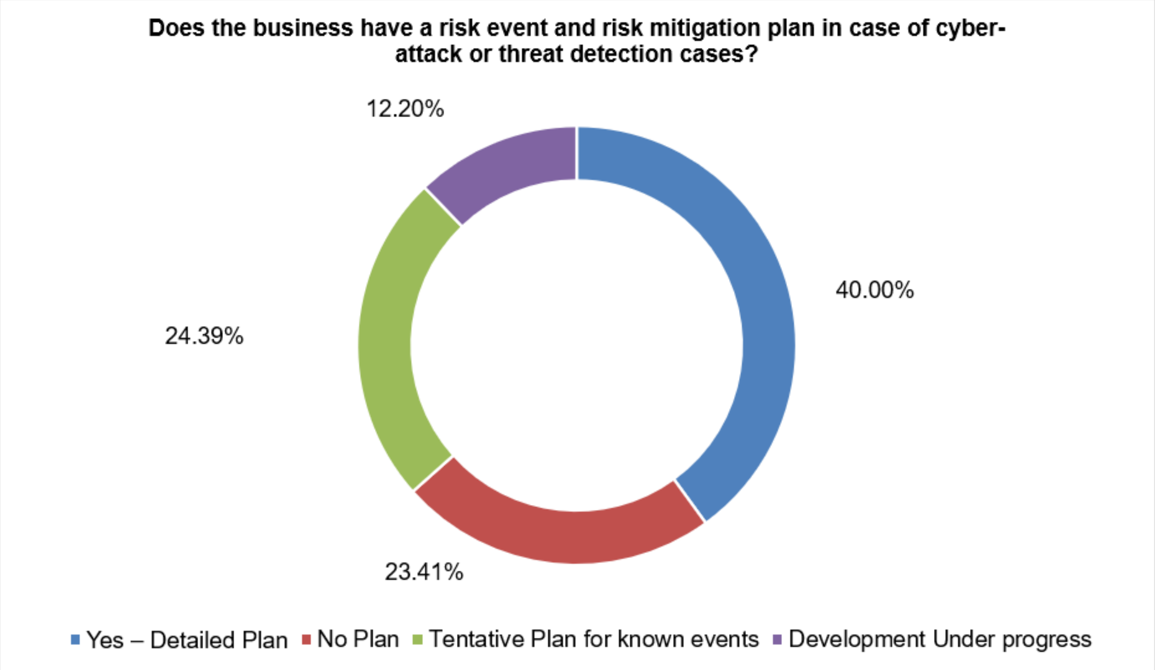


Figure 88

Table 104 shows that 87 of the total survey participants and Figure 89 shows that 42.44% of participants responded that ‘All events and activities are logged’ to monitor user activities.

Table 104: User activity logging on IT infrastructure

Does the business monitor and log user activities?		
User Activity logging	**No. of Responses**	**No. of Responses as % of Total**
Yes – All events and activities are logged	87	42.44%
Logging is separated based on access to application, network, storage, and devices	43	20.98%
Logging is enabled only for data critical applications and storage drives	30	14.63%
Logging is enabled only for identified users and application	25	12.20%
Logging mechanism is separate and not part of IT Security	20	9.76%
Total	**205**	**100.00%**

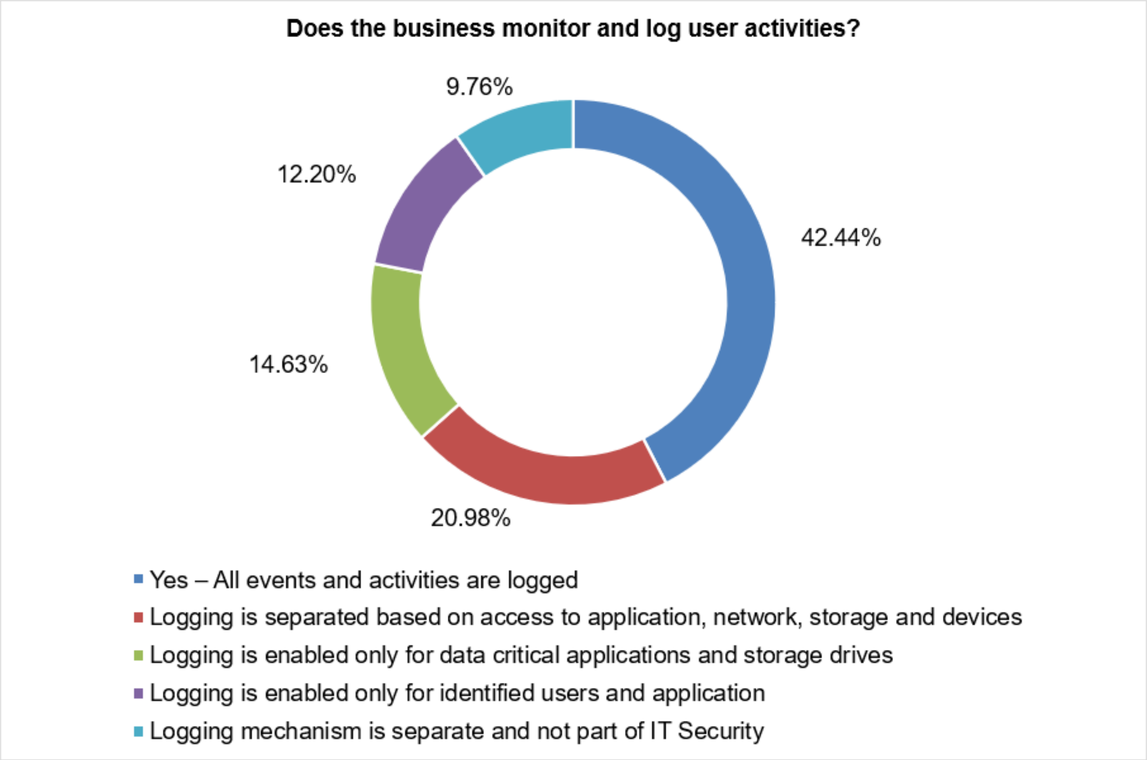


Figure 89

Table 105 shows that 68 of the total survey participants and Figure 90 shows that 33.17% of participants responded that 'Advance tools are in place' in the form of machine learning (ML) and Artificial intelligence (AI) to respond to suspicious activities by internal or external users.

Table 105: Machine learning and artificial intelligence to respond to suspicious activities by internal or external users.

Do you plan, OR have you implemented machine learning (ML) and Artificial intelligence (AI) to respond to suspicious activities by internal or external users?		
ML and AI	**No. of Responses**	**No. of Responses as % of Total**
Yes – Advance tools are in place	68	33.17%
No – No need of such tools	60	29.27%
No - due to Budget constraint	39	19.02%
Plan to implement but no plan or timelines	38	18.54%
Total	**205**	**100.00%**

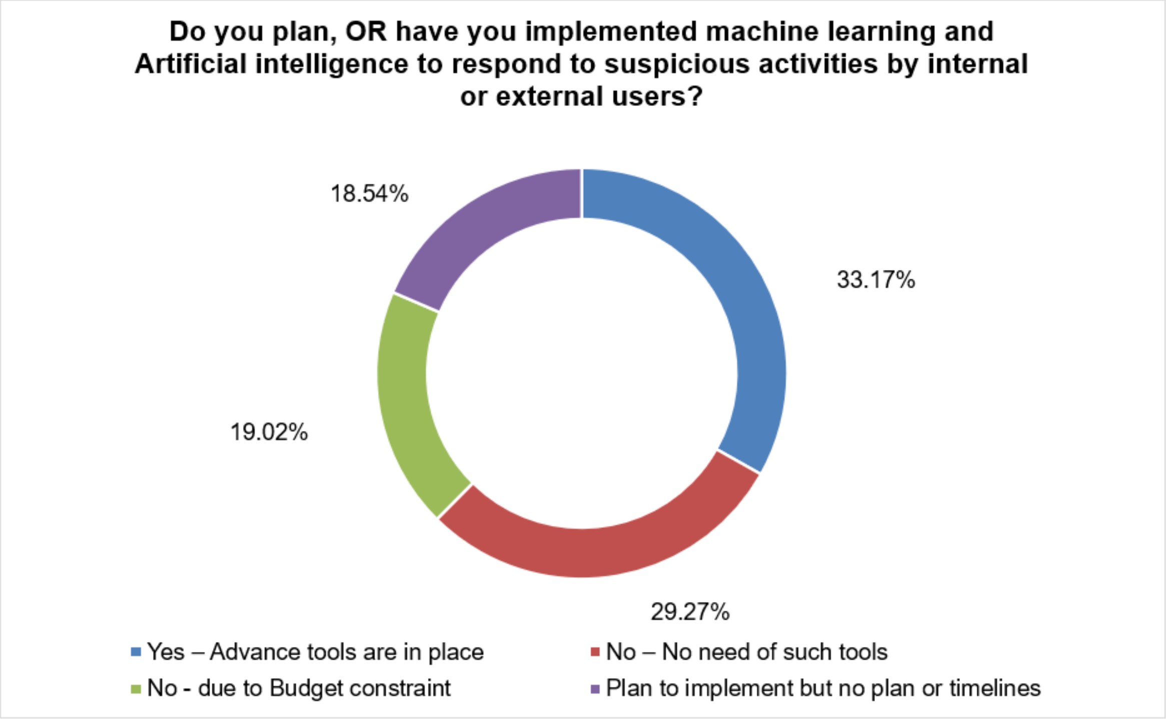


Figure 90

Table 106 shows that 84 of the total survey participants and Figure 91 shows that 40.98% of participants responded that ‘Risk indicators for Server, Applications, storage, connecting devices, and Network devices are defined, monitored, maintained, and managed’ to as key risk parameters for IT Infrastructure (Cloud) resources.

Table 106: Risk parameters for IT infrastructure

Has the business got defined key risk parameters for IT Infrastructure (Cloud) resources?		
Risk Parameter Definition	**No. of Responses**	**No. of Responses as % of Total**
Yes – Risk indicators for Server, Applications, storage, connecting devices, and Network devices are defined, monitored, maintained, and managed	84	40.98%
Yes – Few key risk indicators for cloud infrastructure resources are known	57	27.80%
Yes – Risk indicators are known but there is no central team to manage	28	13.66%
No – All risk indicators are not known; however, responsibility is with cloud service provider	36	17.56%
Total	**205**	**100.00%**

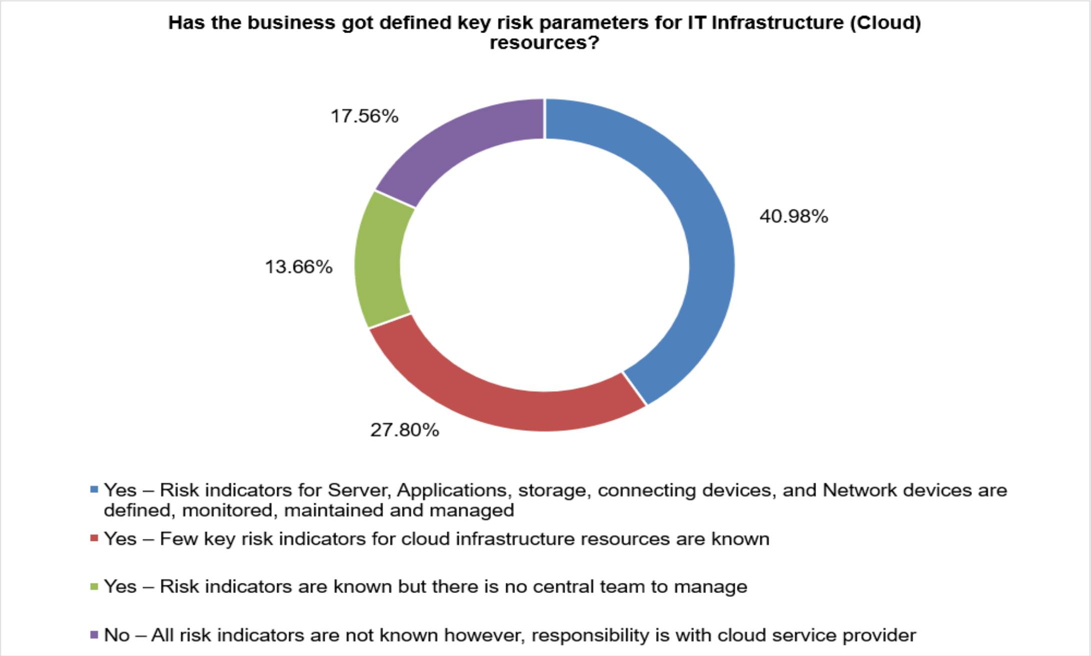


Figure 91

Table 107 shows that 68 of the total survey participants and Figure 92 shows that 33.17% of participants responded that ‘Partial job rotation within team handling sensitive information and tasks’ and similar is response for ‘No job rotation within teams.

Table 107: Job rotation, work culture and IT infrastructure support teams

Is there a job rotation within IT security team?		
Job Rotation, work culture and IT Infrastructure Support Teams	**No. of Responses**	**No. of Responses as % of Total**
Yes – Regular roles and responsibility are changed within team	43	20.98%
Yes – Partial job rotation within team handling sensitive information and tasks	68	33.17%
No – No job rotation within teams	68	33.17%
Organization does not support such actions	26	12.68%
Total	**205**	**100.00%**

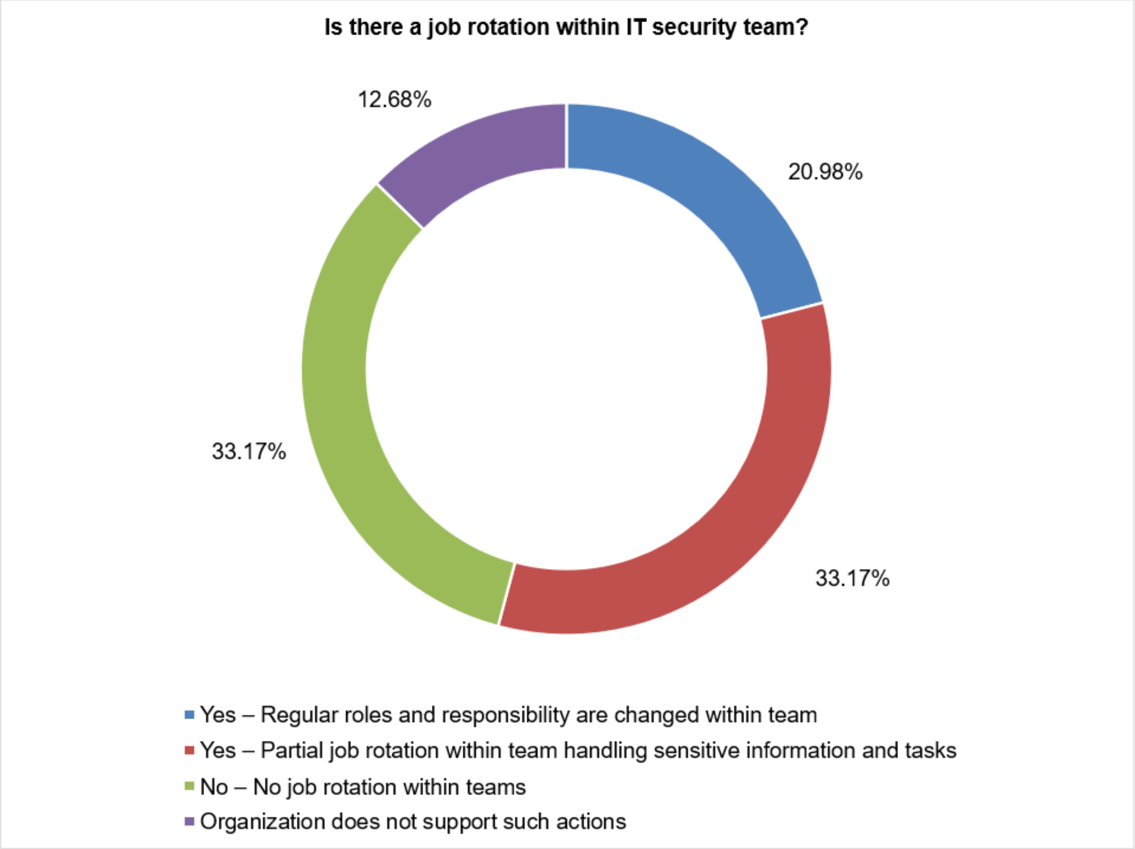


Figure 92

Table 108 shows that 72 of the total survey participants and Figure 93 shows that 35.12% of participants responded that ‘Test and production environment are on same cloud machines however, monitoring and alert mechanism is same for both test and production environment’ is the method to manage test and main / production (live) environments.

Table 108: Development environment management on IT infrastructure (cloud)

How does the business monitor, support, maintain and govern “test / development” environments and main / production live environments over IT Infrastructure (Cloud)?		
Development Environment Management in IT Infrastructure (Cloud)	**No. of Responses**	**No. of Responses as % of Total**
Test and Production are on separate cloud machine and has dedicated monitoring and alert mechanism	68	33.17%
Test and production environment are on same cloud machines however, monitoring and alert mechanism is same for both test and production environment	72	35.12%
Test Environment are not monitored or governed due to low risk	38	18.54%
Test environments are managed internally and not hosted over IT Infrastructure (Cloud)	27	13.17%
Total	**205**	**100.00%**

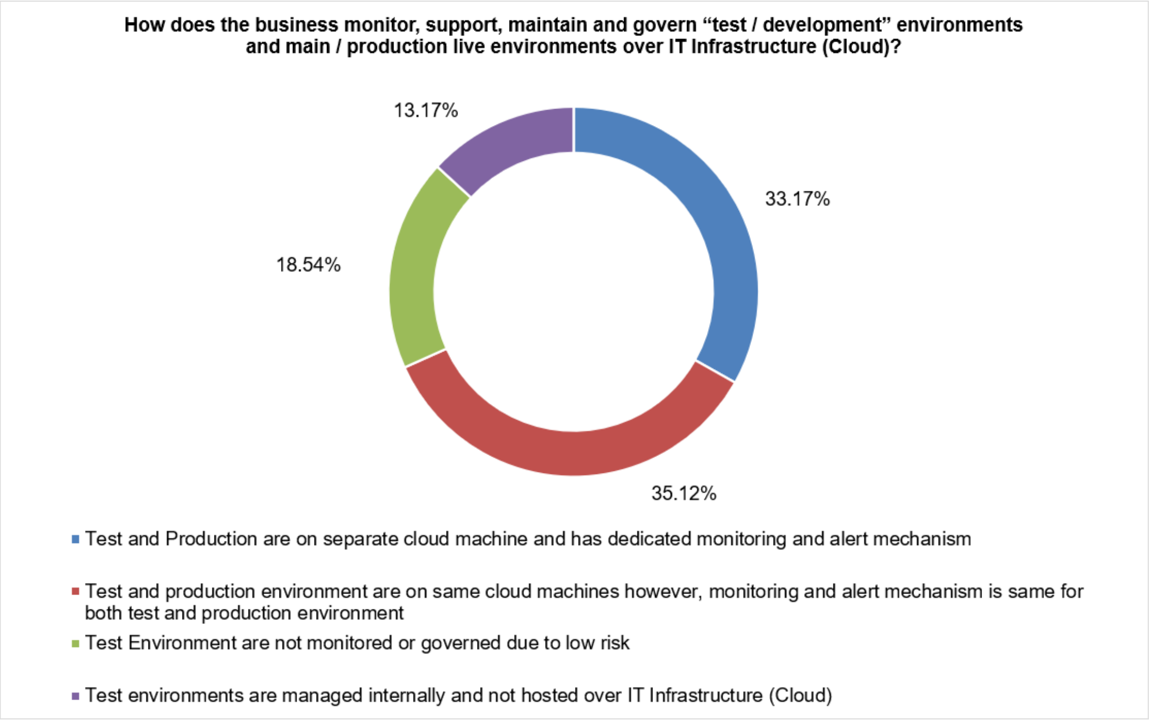


Figure 93

4.2.19 Reflection of research work concerning RQ4

Development of new technical parameter (56.59%) and new IT infrastructure (53.17%) forms key to manage cloud governance for digital transformation. Vulnerability assessment tools is helpful (40.49%) to manage data and system security for digital platforms. Digital transformation has added new data leakages areas (45.37%). Dedicated team required to manage new risk to cloud architecture (28.78%). Cloud governance team (45.85%) with ITIL framework manages emergency changes. IT security plan includes data and system security plans (37.07%). Customer account information (44.39%) key to manage data leakages. Traffic management (37.56%) help to some extent to manage users. Security certificates (SSL) are managed quarterly (24.39%) by 3rd party cloud security providers. Cloud security is upgraded as prescribed by vendors (33.66%). There is need of prescribed risk event and risk mitigation plan (40.00%) in case of cyber-attack or threat detection cases. Artificial intelligence and machine learning are not implemented to respond to suspicious activities by internal or external users however advance tools are implemented for suspicious activities detection and response (33.17%). Risk indicators for cloud are defined (40.98%). There is partial job rotation

(33.17%) or no job rotation (33.17%) within IT security teams. Most companies do not maintain test and main production environment on different cloud infrastructure (35.12%).

4.2.20 Prominent Theme Emerging for RQ4 from survey feedback

The prominent theme emerging from responses received for RQ4 can be categorised in to following:

1. Digital transformation demand investment into new cloud infrastructure.

2. 3rd Party vendor plays key role is managing cloud security

3. Risk event and risk mitigation plans are mandatory

4. Job rotation is required within IT security teams

4.2.21 Discussion of research question 5 (RQ5)

Below table shows linking of RQ5 with survey questions.

Table 109: Linking RQ5 with survey questions.

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
20	How needs of specialised team like Forensic investigation, customer experience platforms, regulatory bodies are addressed through cloud governance?	RQ5	Cloud Governance
15	Do you have process and tools in place to recover hardware and devices in case specific department asks for its?	RQ5	Cloud Security

Table 110: Linking RQ5 with RQ1 and RQ2 survey questions.

Question No. in Questionnaire	Question Description	Research Question No.	Research Area
47	How are you supporting the digital transformation across Bank?	RQ1, RQ2, RQ5	Cloud Security

Table 111: Linking RQ5 with RQ1, RQ2 and RQ4 survey questions.

Question No. in Questionnaire	Question Description	Research Question (RQ) No.	Research Area
34	What are methods for data deletion for lost devices?	RQ1, RQ2, RQ4, RQ5	Cloud Security

Table 112: Linking RQ5 with RQ1, RQ2, RQ3 and RQ4 survey questions.

Question No. in Questionnaire	Question Description	Research Question (RQ) No.	Research Area
44	Are IT Security contracts separate from Enterprise IT Contracts?	RQ1, RQ2, RQ3, RQ4, RQ5	Cloud Security

The column “Question No.” in above table shows the sequence number in actual questionnaire emailed to participants.

Table 113 shows that 100 of the total survey participants and Figure 94 shows that 48.78% of participants responded that ‘Need based engagement by IT infrastructure (Cloud) Support team’ is the method to fulfill needs of specialised team like computer forensic investigation, customer experience platforms, regulatory bodies, Audits addressed through IT infrastructure (Cloud) management / governance.

Below shows the responses received for RQ5 from survey Participants:

Table 113: Digital forensic and IT infrastructure

How are the needs of specialised team like computer Forensic investigation, customer experience platforms, regulatory bodies, Audits addressed through IT infrastructure (Cloud) management / governance?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Dedicated Team(s) to handle each of these areas	87	42.44%
Need based engagement by IT infrastructure (Cloud) Support team	100	48.78%
Others (specify)	2	0.98%
None of these	16	7.80%
Total	**205**	**100.00%**

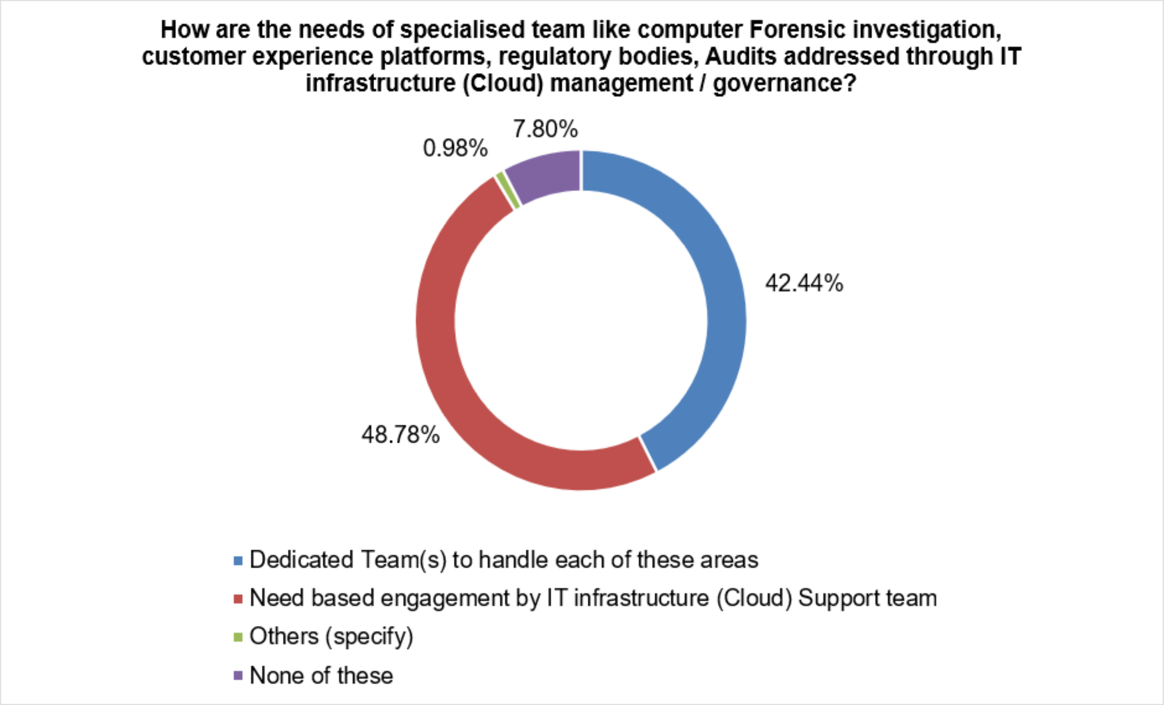


Figure 94

Table 114 shows that 150 of the total survey participants and Figure 95 shows that 73.17% of participants responded that business have process and tools in place to recover hardware and devices in case specific department requests.

Table 114: Specific tools for data recovery

Does the business have process and tools in place to recover hardware and devices in case specific department asks for it?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Yes	150	73.17%
No	27	13.17%
Unsure	28	13.66%
Total	**205**	**100.00%**

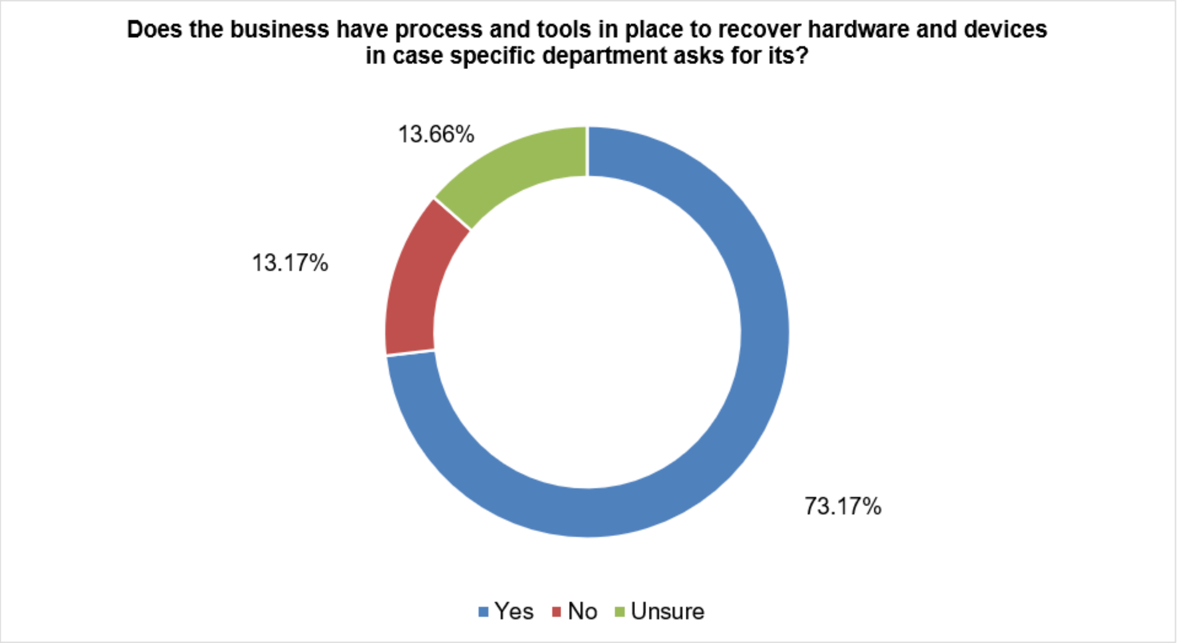


Figure 95

Table 115 shows that 90 of the total survey participants and Figure 96 shows that 73.17% of participants responded that ‘Lost devices are isolated and monitored for further investigation’ (followed by ‘Lost devices are de-activated permanently from network connectivity’) and is a method used for data control over lost devices.

Table 115: Data deletion for data loss prevention

What methods are used for data deletion for lost devices?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Lost devices are de-activated permanently from network connectivity	87	42.44%
Lost devices are isolated and monitored for further investigation	90	43.90%
Devices other than laptop devices are not allowed to be used over IT Infrastructure (Cloud)	47	22.93%
No process to remove data from lost devices	37	18.05%
Total	**205**	**100.00%**

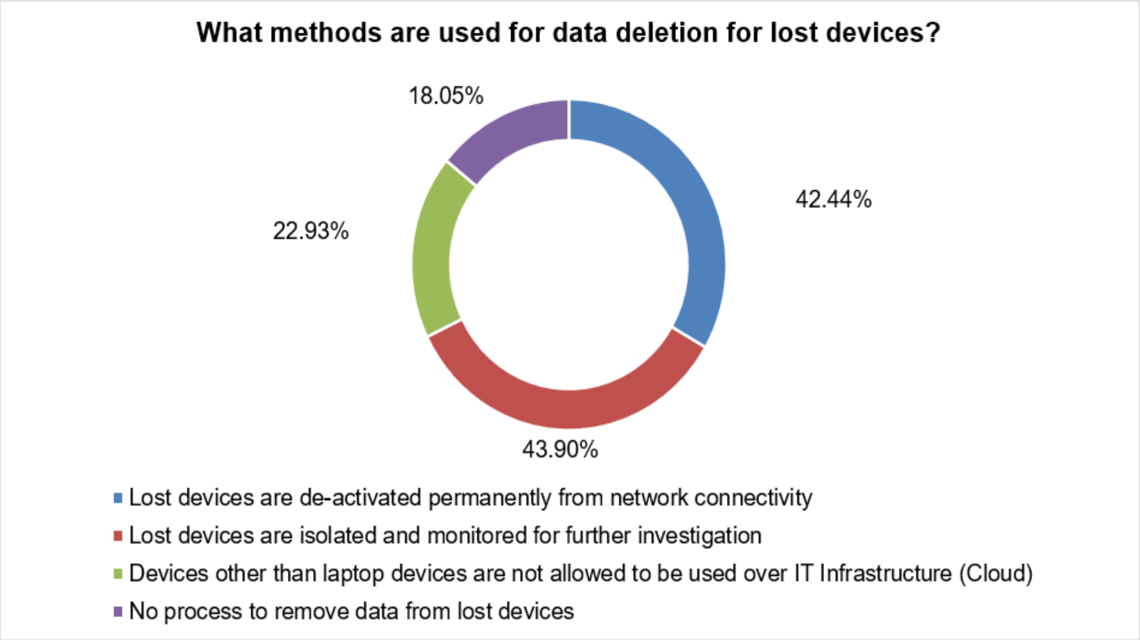


Figure 96

Table 116 shows that 68 of the total survey participants and Figure 97 shows that 33.17% of participants responded that ‘IT Security contracts are carefully written to meet security specific needs of the company’ and is the method to separate IT contracts with Company / Bank / Enterprise IT Contracts.

Table 116: IT security contract and IT cloud infrastructure

Are IT Security contracts separate from Company / Bank / Enterprise IT Contracts?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Yes – IT Security contracts are carefully written to meet security specific needs of the company	68	33.17%
IT Security Contracts are like overall enterprise IT contracts	43	20.98%
IT Security contracts are closely coupled with each Enterprise IT contracts	28	13.66%
IT security contracts are loosely coupled with enterprise contract based on needs	27	13.17%
Unsure	39	19.02%
Total	**205**	**100.00%**

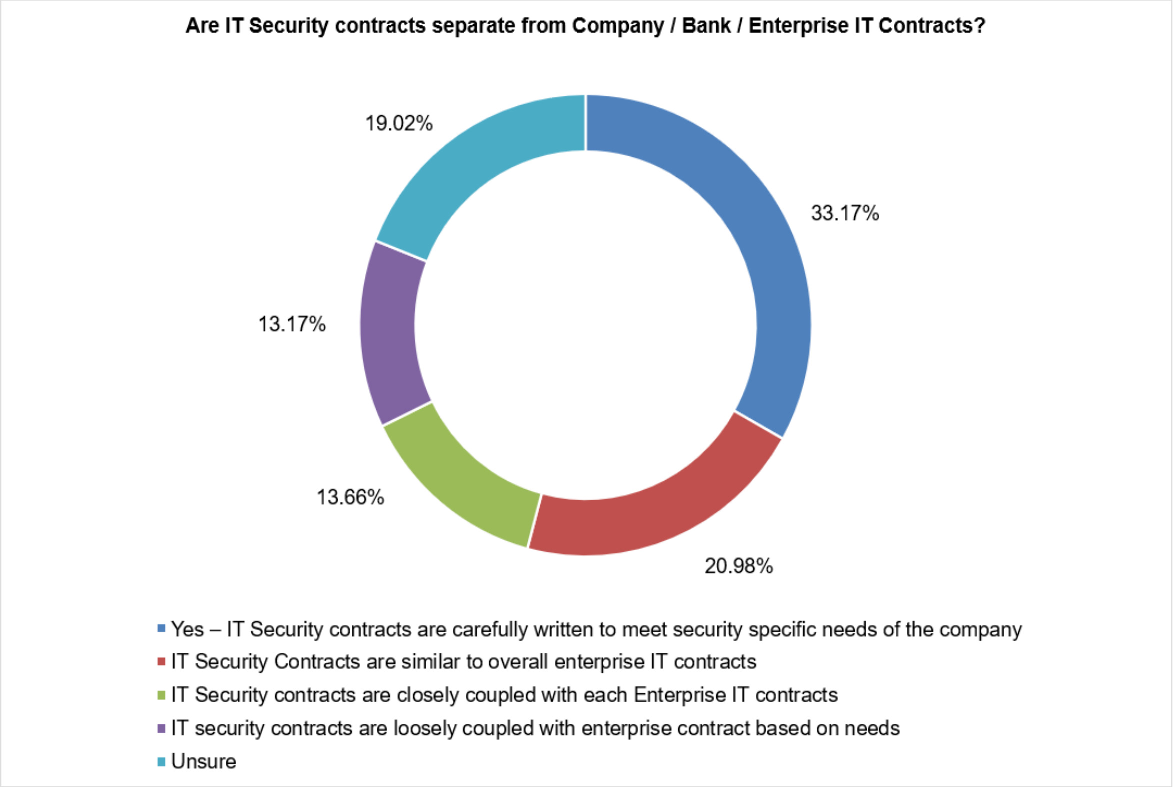

Are IT Security contracts separate from Company / Bank / Enterprise IT Contracts?
19.02%
33.17%
13.17%
13.66%
20.98%
Yes – IT Security contracts are carefully written to meet security specific needs of the company
IT Security Contracts are similar to overall enterprise IT contracts
IT Security contracts are closely coupled with each Enterprise IT contracts
IT security contracts are loosely coupled with enterprise contract based on needs
Unsure

Figure 97

Table 117 shows that 67 of the total survey participants and Figure 98 shows that 32.68% of participants responded that ‘Passively involved in discussions and ongoing implementation as digital transformation is handled by 3rd Party’ is the method to support digital transformation across companies.

Table 117 shows that 65 of the total survey participants and Figure 98 shows that 31.71% of participants responded that ‘Digital transformation unit independently supports needs from cloud security perspective’.

Table 117 shows that 63 of the total survey participants and Figure 98 shows that 30.73% of participants responded that ‘Actively participating to provide security solutions required for digital platform’.

Table 117: Digital transformation and IT infrastructure

How are you supporting the digital transformation across companies?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Actively participating to provide security solutions required for digital platform	63	30.73%
Digital transformation unit independently supports needs from cloud security perspective	65	31.71%
Passively involved in discussions and ongoing implementation as digital transformation is handled by 3rd Party	67	32.68%
Digital transformation platform are hosted on 3rd Party cloud services and not part of Bank’s (and companies) IT Infrastructure (Cloud) infrastructure	41	20.00%
Digital transformation is not a Bank’s priority currently	19	9.27%
Unsure	34	16.59%
Total	**205**	**100.00%**

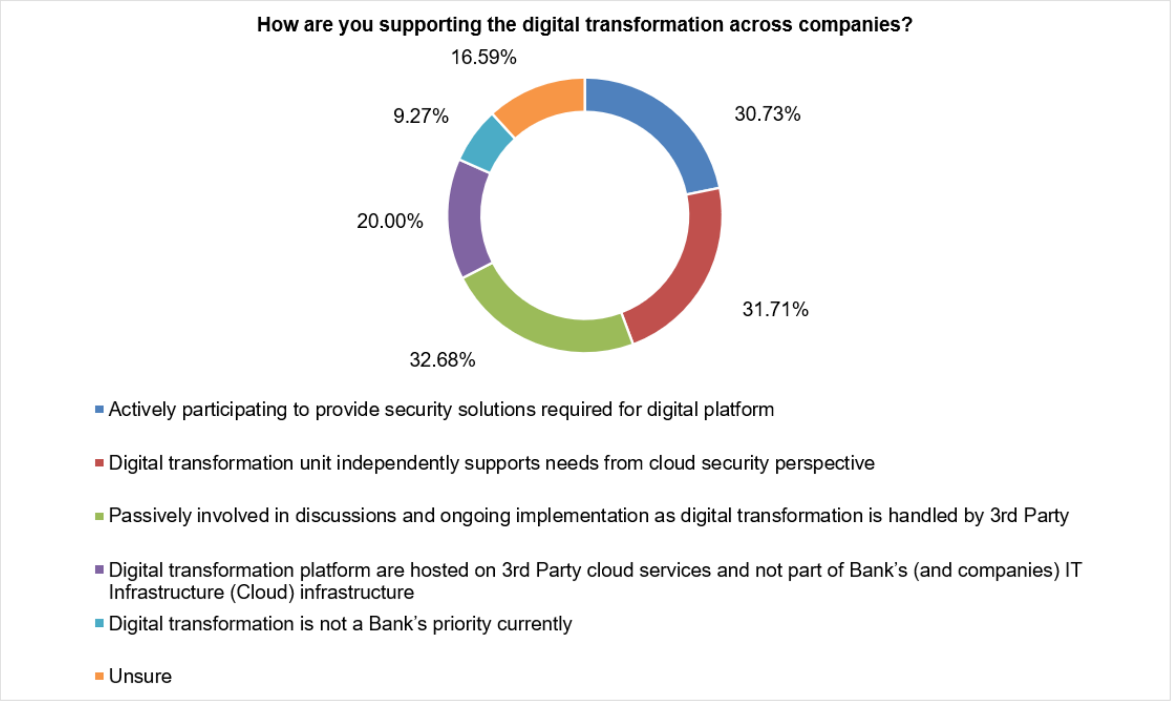


Figure 98

4.2.22 Reflection of research work concerning research question 5 (RQ5)

Engagement with computer forensic teams is need based (48.78%). There are specific process and tools (73.17%) in place to recover hardware and devices in case specific department required. Devices which are lost are managed through isolation (43.90%). IT security contracts are separate than cloud contracts (33.17%). Most people are actively (30.73%) or passively (32.68%) supporting digital transformation with independent teams implementing digital transformation (31.71%).

4.2.23 Prominent Theme Emerging for Research Question 5 (RQ5) from survey feedback

The prominent theme emerging from responses received for RQ5 can be categorised in to following:

1. There is a need of specific tools and people to manage specific investigations

2. IT Security contract needs special handling.

4.3 Discussion of Interview Questionnaire

Below are areas captured through survey-cum-interview questions:

Table 118: Interview questions on cloud perception

Question No.	Question Description	Interview Question No.	Research Area
1	Ease of Use	1	Cloud Perception
2	Flexibility to work from Home	2	Cloud Perception
3	Data confidentiality and information security maintained	3	Cloud Perception
4	Simple to connect	4	Cloud Perception
5	Availability of all computing resources	5	Cloud Perception
6	Secure to connect from private network	6	Cloud Perception
7	Ability to recover data in case of loss	7	Cloud Perception
8	Support from remotely located teams in case of incidents	8	Cloud Perception

Below are responses received for interview questions:

Table 119: Ease of use of IT infrastructure (cloud)

How easy is to use are the IT Infrastructure (Cloud) services? (Rate from 1 to 5, 5 = Very Easy, 1 = Very Difficult)		
Response	**No. of Responses**	**No. of Responses as % of Total**
1 - Very easy	17	8.29%
2	52	25.37%
3	83	40.49%
4	38	18.54%
5 - Very difficult	15	7.32%
Total	**205**	**100.00%**

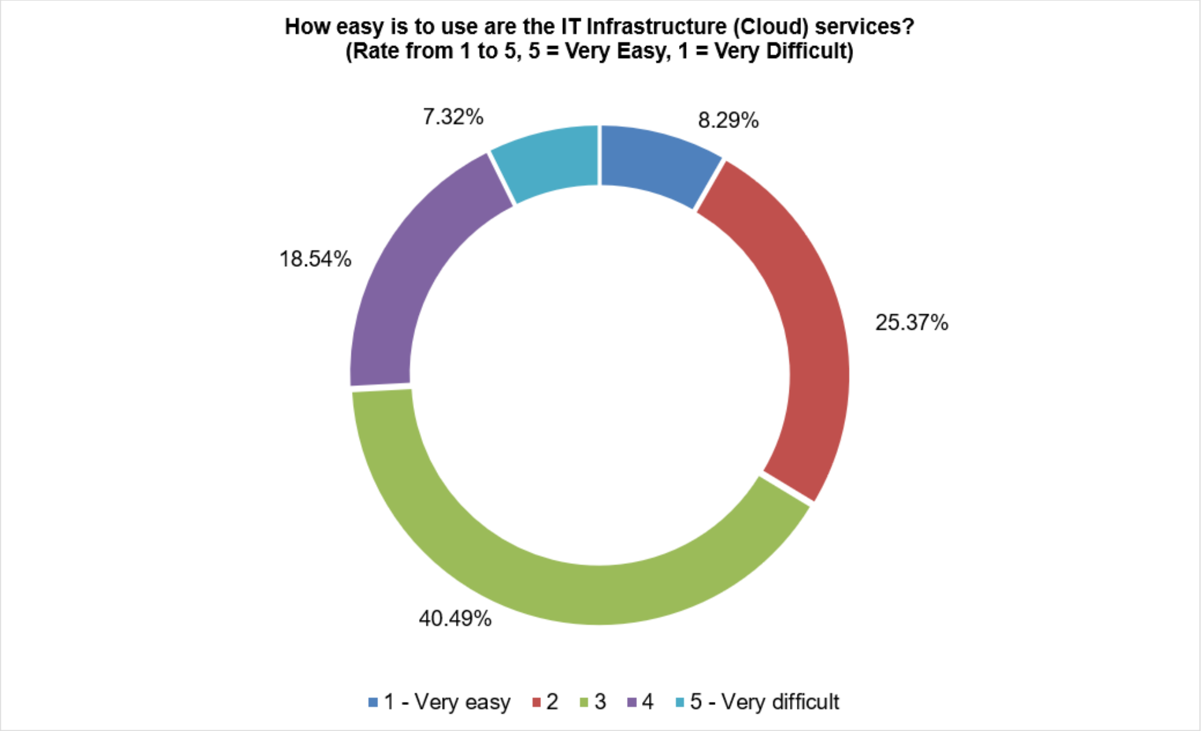


Figure 99

Table 120: Flexibility to work from home.

Does IT Infrastructure (Cloud) services truly provide flexibility to work from home? (Rate from 1 to 5, where 1 = Very Inflexible and 5 = Very Flexible)		
Response	**No. of Responses**	**No. of Responses as % of Total**
1 - Very inflexible	5	2.44%
2	15	7.32%
3	68	33.17%
4	70	34.15%
5 - Very flexible	47	22.93%
Total	**205**	**100.00%**

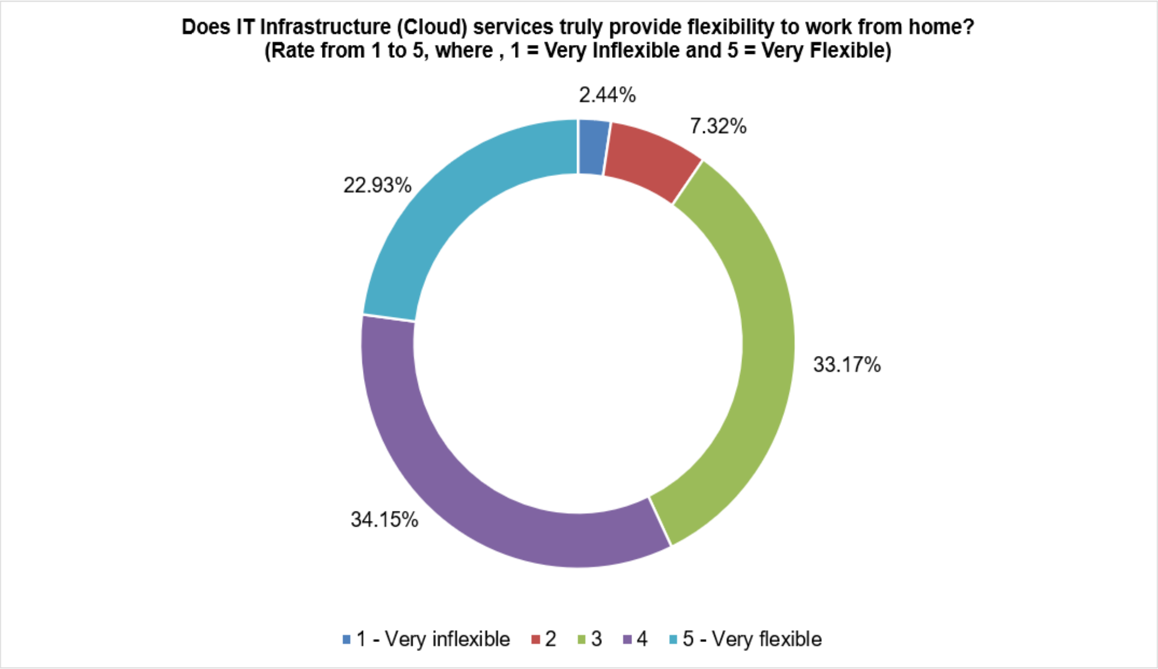


Figure 100

Table 121: Data confidentiality and information security maintained.

Do you think IT Infrastructure (Cloud) helps to maintain data confidentiality and information security?		
Response	**No. of Responses**	**No. of Responses as % of Total**
1 - Poor Confidentiality and Security	4	1.95%
2	18	8.78%
3	68	33.17%
4	88	42.93%
5 - Very Confidential and Secure	27	13.17%
Total	**205**	**100.00%**

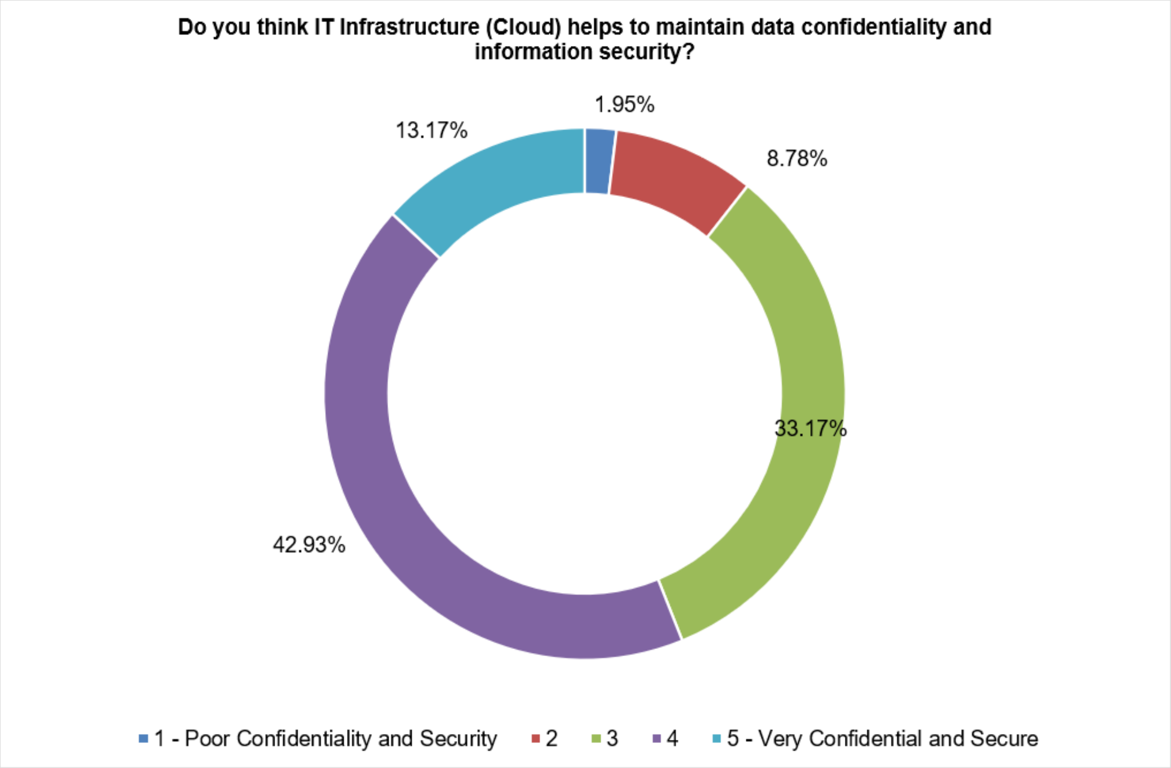


Figure 101

Table 122: Simple to connect.

How easy is it to connect IT Infrastructure (Cloud) services? (Rate from 1 to 5, where 1 = Very Difficult and 5 = Very Easy)		
Response	**No. of Responses**	**No. of Responses as % of Total**
1 - Very difficult	0	0.00%
2	13	6.34%
3	63	30.73%
4	86	41.95%
5 - Very easy	43	20.98%
Total	**205**	**100.00%**

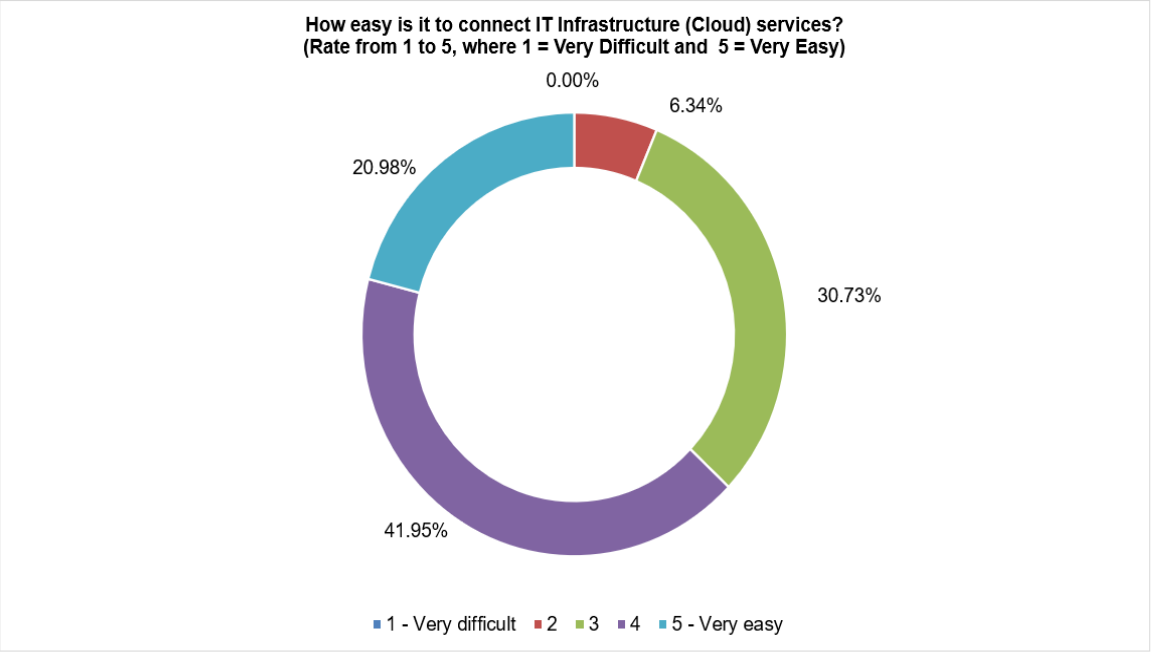


Figure 102

Table 123: Availability of all computing resources

Can you access all the IT Infrastructure (Cloud) / computing resources available via IT Infrastructure?		
Response	**No. of Responses**	**No. of Responses as % of Total**
1	2	0.98%
2	15	7.32%
3	58	28.29%
4	90	43.90%
5	40	19.51%
Total	**205**	**100.00%**

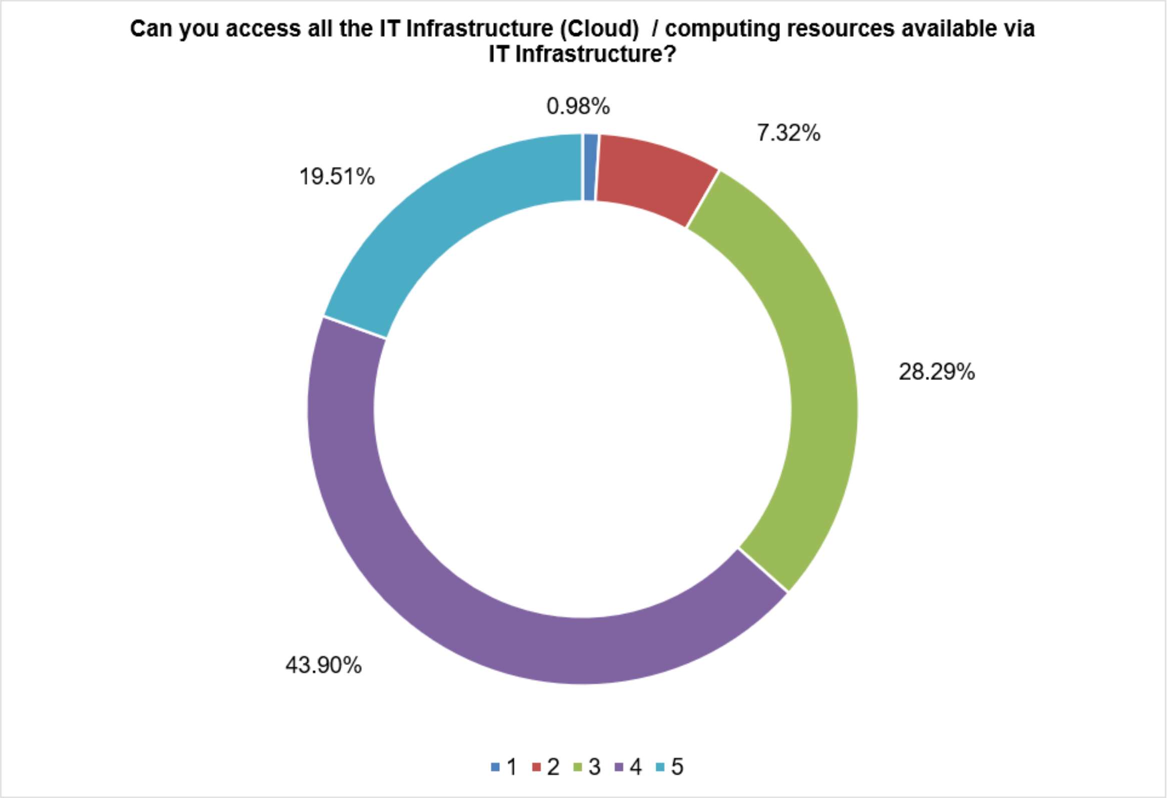


Figure 103

Table 124: Secure to connect from private network.

Do you think it is secure to connect to IT Infrastructure (Cloud) from private / home internet? (Rate from 1 to 5, where 1 = Not Secure at All and 5 = Very Secure)		
Response	**No. of Responses**	**No. of Responses as % of Total**
1 - Not secure at all	4	1.95%
2	15	7.32%
3	67	32.68%
4	85	41.46%
5 - Very secure	34	16.59%
Total	**205**	**100.00%**

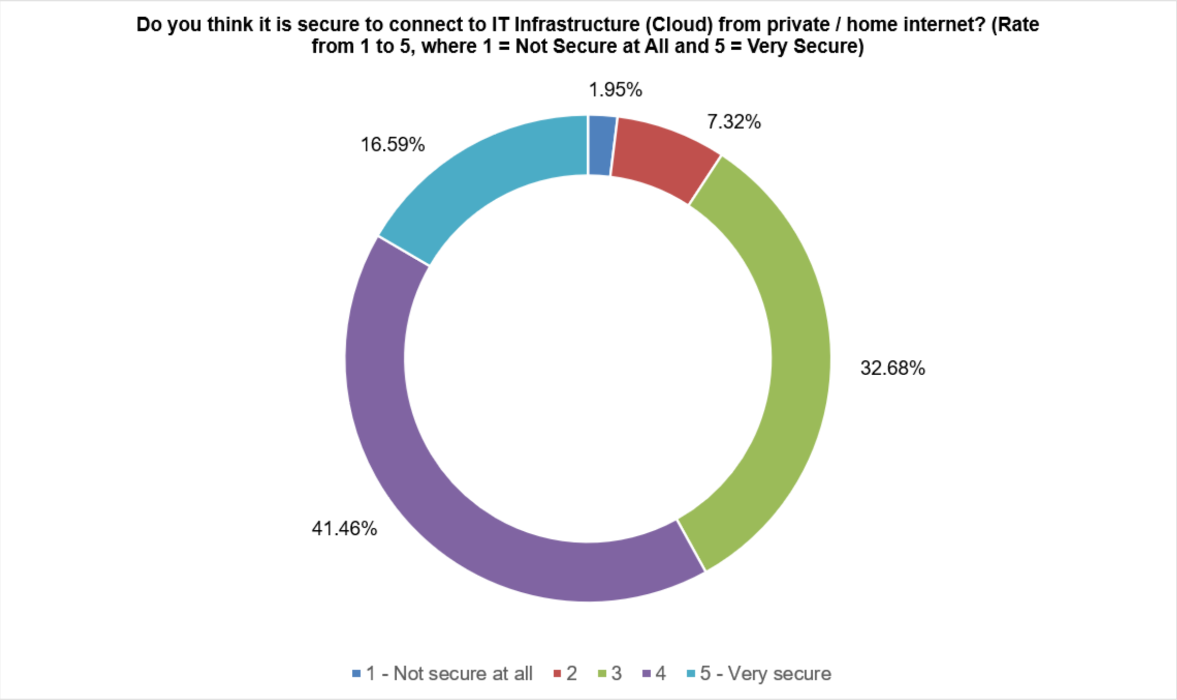


Figure 104

Table 125: Ability to recover data in case of loss.

If any data is lost due loss of connectivity, do you get this recovered?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Yes	153	74.63%
No	52	25.37%
Total	**205**	**100.00%**

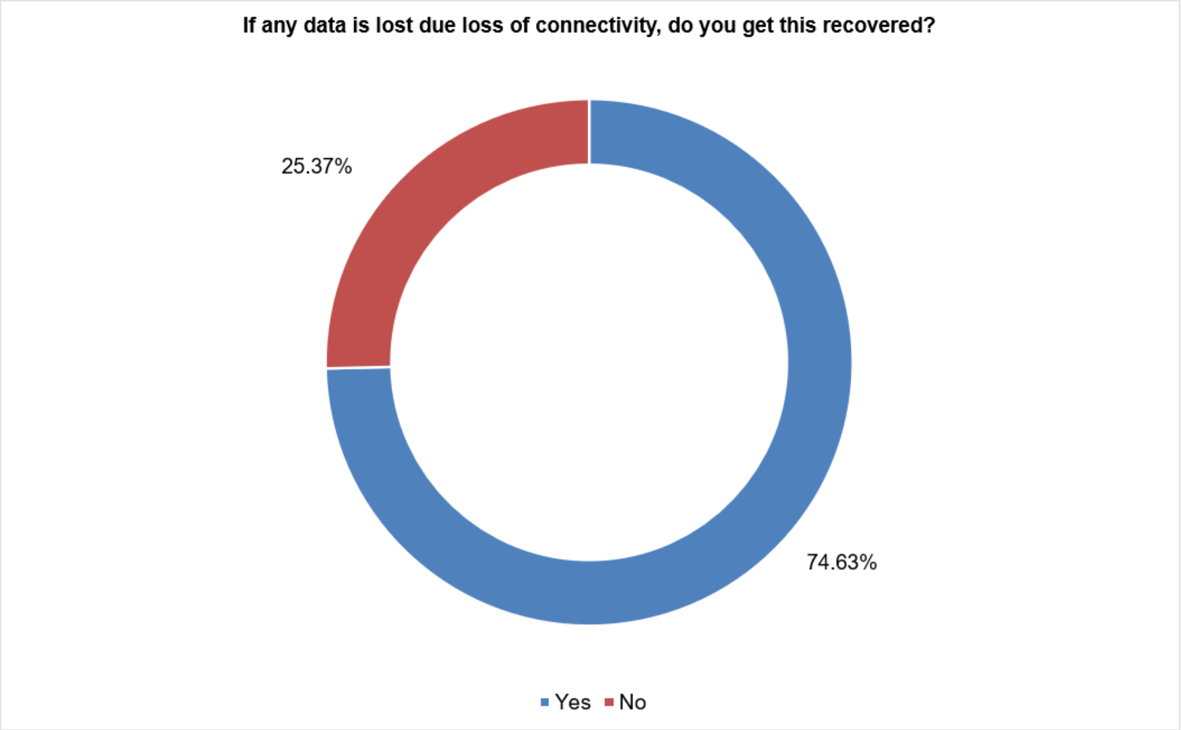


Figure 105

Table 126: Support from remotely located teams in case of incidents.

Is there any support from remotely located teams in case of incidents?		
Response	**No. of Responses**	**No. of Responses as % of Total**
Yes	149	72.68%
No	56	27.32%
Total	**205**	**100.00%**

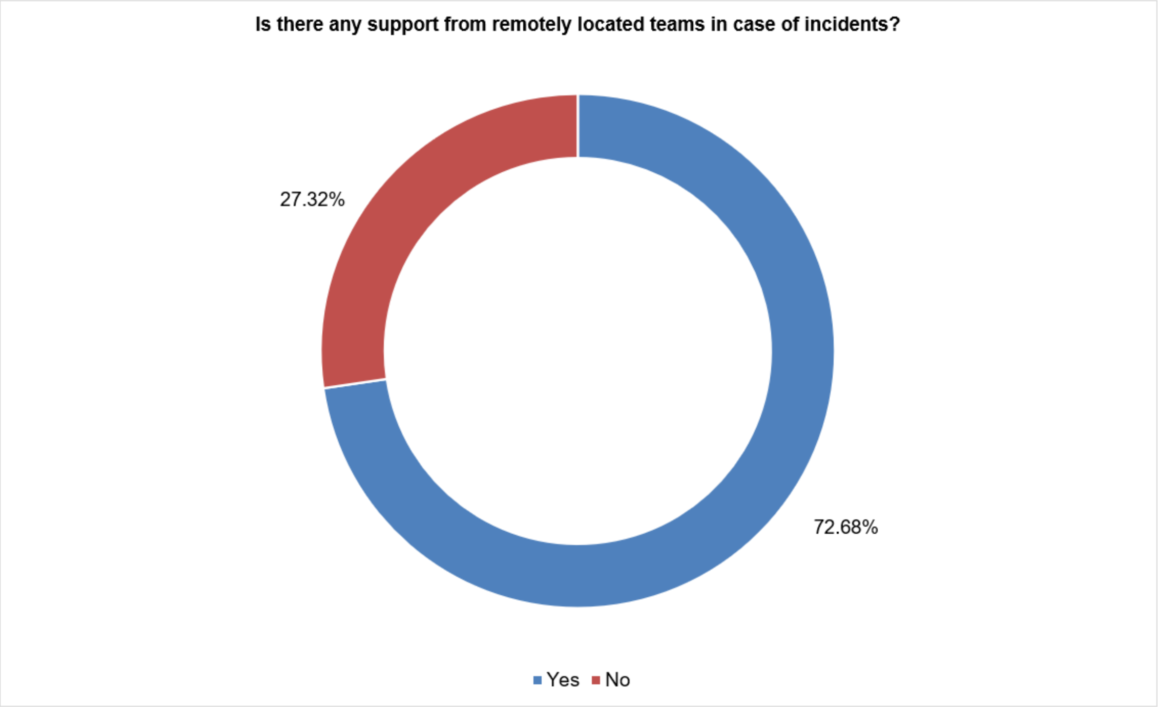


Figure 106

4.3.1 Reflection of Research Work concerning Interview Questionnaire

Using cloud infrastructure has medium level of complexity (40.49%). Cloud infrastructure is good help in case of "work from home" scenario offering flexibility of work (34.15%). IT Infrastructure (Cloud) helps to maintain data confidentiality and information security (42.93%). It is complex to connect to cloud infrastructure (41.95%). Most resources on cloud are accessible (43.90%). It is not secure to connect cloud infrastructure from home (41.46%). Data lost due to connectivity is recovered (74.63%). Remotely located team support incident over cloud (72.68%).

4.3.2 Prominent Theme Emerging from Interview Questionnaire

The prominent theme emerging from responses received for RQ5 can be categorised in to following:

1. It is complex to connect to cloud infrastructure.

2. Cloud infrastructure connectivity offers flexibility, data confidentiality, information security, availability of computing resources

3. Cloud infrastructure posses security challenges when connecting from home / remote location.

4.4 Chapter Summary

This chapter listed the organization of the survey and interview questions. This chapter provided the detailed responses received from survey and interview participants for the survey completed. This chapter summarised the major findings from the survey for each research questions. This chapter discussed and provided emerging themes out of research findings.

CHAPTER 5: CONCLUSION

5.1 Chapter introduction

This chapter provides a conclusion to this thesis with a summary of the key research findings to demonstrate how this research has met its objectives. This is followed by an account of the contributions of the research to theory and practice. This chapter is organised into six sections. This section is an introduction to the final chapter. A summary of the research findings is provided in *section 5.2*. The contributions this research makes to theory and practice are presented in *section 5.3*. Limitations of the research are provided in *section 5.4*. Directions for future research are suggested in *section 5.5*. The final chapter summary is provided in *section 5.6*.

5.2 Summary of research findings

The study answers the five research questions:

RQ1: What will be the impact to the various data categories and application types used by Banking and Financial Services Corporations due to cloud architecture and how it will impact the business and customers?

This research answers that in managing data categories and application types is complex over cloud architecture. To manage this complexity cloud architecture and infrastructure continue to demand investment. The data categories identified currently by Banks must be interrelated to identify new creative method to breach privacy. The data under these data categories when lost will have potential impact on customers in terms its misuse in near future, inconvenience to customers and discomfort. The applications processing these data categories, will not provide accurate output leading to illogical processing of data and application & information corruption. Due to cloud architecture, the loss of data categories and applications will disrupt business activities leading to monetary loss to banks and will invite penalty from regulator.

RQ2: What type of measures and controls will be required for cloud computing architecture for Banking and Financial Services Corporations to enforce data privacy and system security?

This research answers that to enforce data privacy and system security dedicated incident and problem management team, legal expertise to form cloud management contracts, dedicated team for managing cloud security penetration testing teams, dedicated human resources with relevant work experience, IT Risk management framework and alert & monitoring for ongoing use of cloud infrastructure will be required to measure and control cloud computing architecture and infrastructure. The various teams identified will have to work closely with each other for service orchestration to demonstrate overall working method and control over cloud architecture. Developing central team with variety of knowledge and skill about various aspects technical and commercial aspects of cloud architecture can provide control and enforce protocols required to enforce privacy and system security.

RQ3: What will be the role of cyber security executives, security framework and governance structure to improve cloud security **of banking and financial services corporations***?*

This research answers that roles and responsibility of cyber security executives along with security framework and governance structure will be required to review quarterly. Dedicated budget, business continuity plans and ethical controls will be required within cyber security teams. Job rotation is required within cyber security executives. Cyber security executives must be continuously educated about recent cyber-attacks and potential losses incurred by other organizations; this will help relate exiting cyber security framework with threats identified, deploy additional resources, and keep banks future ready for new cyber-attacks. Considering nature, intensity, sensitivity, risk, role and accountability in cyber security domain, supports from Bank's leadership is required to enforce string security protocols.

RQ4: What will be risks to customer data due to digital transformation in Banking and Financial Services Industry?

This research answers that Digital transformation demand investment into new cloud infrastructure to prevent data leakages risk to customer data. 3rd Party cloud service providers plays a key role in managing cloud security. Risk event and risk mitigation plans are mandatory for digital transformation. Digital transformation involving 3rd party cloud service provider brings the aspects of shared responsibility to secure cloud. The technical architecture of digital platforms within cyber security perimeter and round the clock availability of Bank's digital platform demands continuous monitoring to prevent cyber-attacks and take necessary actions to block such cyber-attacks to prevent loss customer data.

RQ5: How will cloud architecture support need of specific departments from bank for forensic investigation purposes **of banking and financial services corporations***?*

This research answers that there is need of specific tools and people to manage specific forensic investigations. This research also suggests that IT Security contract needs special handling in special investigation scenarios. To support digital forensic investigation that demand securing exiting and historical data, bank need to set up dedicated on demand data providers, data recovery tools and files access mechanism within cyber security team. The timeframe required to secure digital data needs to be adhered to ensure timely investigation and action. The cyber security leader of the bank to handle the investigation related to such confidential incidents.

5.3 Link of publications and research findings

This section presents the connections between published works and conclusion reported in the thesis.

5.3.1 Publication 1 & 8 and RQ1:

Publication 1: Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure, 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, China

Publication 8: Challenges and Mitigation for Application Deployment over SaaS Platform in Banking and Financial Services Industry, IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China

Linked Research Question: RQ1

Description of Linkage: Research outcome for RQ1 confirms the complexity, need and risk to various data categories stored on cloud architecture and cloud infrastructure for Banking and Financial Services Corporations. These publications provide various types of data and application that are at hosted on cloud infrastructure along with risk & mitigation plan. These publications detail various data and applications (their development, maintenance and risk management) that will demand financial investment to prevent data loss.

5.3.2 Publication 2 & 6 and RQ2

Publication 2: ITIL Processes to Control Operational Risk in Cloud Architecture Infrastructure for Banking and Financial Services Industry, 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC), Kaohsiung, Taiwan

Publication 6: IT Investment Governance and Corporate Governance: Perspective and Approach, 7th International Conference on Behavioural and Social Computing (BESC), Bournemouth, UK

Linked Research Question: RQ2

Description of Linkage: Research outcome for RQ2 confirms the incident and problem management team, legal expertise to form cloud management contracts, dedicated team for managing cloud security penetration testing teams, dedicated human resources with relevant work experience, IT Risk management framework and alert & monitoring for ongoing use of cloud infrastructure will be required to measure and control cloud computing architecture and infrastructure. These publications provide various teams working in ITIL framework and methods in ITIL that will be required to control operation risk in cloud infrastructure. These publications provide investment and corporate governance guidelines while working with cloud infrastructure.

5.3.3 Publication 3 and RQ2, RQ3

Publication 3: Insider Threat and Mitigation for Cloud Architecture Infrastructure in Banking and Financial Services Industry, 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal

Linked Research Question: RQ2 and RQ3

Description of Linkage: Research outcome for RQ2 confirms the ITIL processes for operational control and risk mitigation for cloud infrastructure. Research outcome for RQ3 confirms roles and responsibility of cyber security executives, dedicated budget, business continuity plans and ethical controls required within cyber security teams. This publication provides the need of governance control framework and development of human resources to mitigate risk to cloud infrastructure.

5.3.4 Publication 4 and RQ2, RQ 3

Publication 4: Ethics of IT Security Team for Cloud Architecture Infrastructure in Banking and Financial Services Industry, 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal

Linked Research Question: RQ2 and RQ3

Description of Linkage: Research outcome for RQ2 confirms the ITIL processes for operational control and risk mitigation for cloud infrastructure. Research outcome for RQ3 confirms roles and responsibility of cyber security executives, dedicated budget, business continuity plans and ethical controls required within cyber security teams. This publication provides specific human behaviour and conduct required to work on cloud infrastructure considering the outcome of RQ2 and RQ3. This publication provides human traits required to govern cloud infrastructure.

5.3.5 Publication 5 & 7 and RQ1, RQ2, RQ4

Publication 5: Protecting Privacy in Digital Era on Cloud Architecture for Banking and Financial Services Industry, 6th International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC), Beijing, China

Publication 7: Regulatory Challenges and Mitigation for Account Services Offered by FinTech, 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China

Linked Research Question: RQ1, RQ2, RQ4

Description of Linkage: Research outcome for RQ1 confirms the complexity, need and risk to various data categories stored on cloud architecture and cloud infrastructure for Banking and Financial Services Corporations. Research outcome for RQ2 confirms the ITIL processes for operational control and risk mitigation for cloud infrastructure. Research outcome for RQ4 confirms investment required for digital transformation to prevent data leakages risk to customer data and role of 3rd Party cloud service providers. These publications provide areas of loss of privacy breach and method to control loss of privacy. These publications provide method to control loss of privacy in digital platforms and regulatory assessment required to delivery technology services delivered by cloud infrastructure.

5.4 Research contribution

This section presents significant contributions claimed by this research to the knowledge base. The research investigated a specific need within organization to manage cloud infrastructure. Hence, the research holds significance for both academia and practice. This research identified key requirements to govern cloud infrastructure.

5.4.1 Contribution to theory and literature

The contribution offered in this research includes specific risks arising due to cloud infrastructure. This research provides theory and literature additional areas previously unidentified to deliver quality and services of cloud computing resources.

5.4.2 Contribution to industry and practice

From a practical standpoint, this research has features to collect assessment data, measure process capability, and provide process improvement recommendations. This research demonstrated how this survey can be applied in practice by developing detailed plan to manage cloud computing resources. Furthermore, a practitioner could use the results of this survey to assess cloud services, cloud security, human resources, and financial budget allocation to improve cloud architecture and cloud infrastructure.

5.5 Limitation of the research

The limitation of the research is defined in the literature review protocol (Chapter 2) resulted in the exclusion of literature that did not meet the predefined criteria. It is possible that relevant research is available in literature from non-English academic studies, business process improvement discipline. The case study in this research included certain limitations. First, regarding internal validity, evaluation data were collected using qualitative research methods. Quantitative methods, in this research it is a survey with the expectations from cloud architecture and cloud infrastructure assessments, which could have provided a broader view on the topic. However, the qualitative case study method is well-suited to study process-related challenges in an organizational context. Additionally, a rich set of data sources was used to build a detailed view of the IT organization and its process culture. Nevertheless, a recognised limitation of the qualitative case study approach is the lack of ability to generalise the findings.

Concerning case selection and external validity, the case study organizations, “prominent bank in Queensland”, was part of research project. Thus, convenience sampling, a generally accepted way to recruit case organizations, was used as a sampling strategy. The case study organizations were required to be in proximity in order to conduct this research. Future research using parametric sampling and more powerful statistical analysis could be conducted.

This research reviewed the risk areas of the case study organizations. A larger number of cases and comparison between other organizations based on diverse evaluation factors would have increased the quality of the case study research. The IT service managers in the single case study provided positive feedback; however, whether this artefact contributes to actual service improvements is beyond the scope of evaluation.

5.6 Directions for future research

The construction of the research in terms of cloud parameters and technological rules are first steps in the process of developing more comprehensive bodies of knowledge or theories. This research proposed a set of parameters to improve cloud risk parameters that is an initial step in the development of a data privacy and system security theory. Several future research directions can therefore be proposed from this Research. Future research should explore feedback cycles from several other areas of cloud computing and cloud security. This research can act, for example, as a pilot case study for further studies. A direction for future research would be to undertake empirical studies on other aspects of cloud computing like cloud storage efficiency, cloud network capabilities. Another consideration for future research is to continue to investigate how the proposed findings of this research can be implemented and their outcome.

5.7 Chapter summary

This research achieved synergy between theory and practice by drawing on academic and practitioner literature and collaborating with academia and industry for data privacy and system security. This chapter provided answers to research questions. This chapter provided contribution to theory literature and practice. This chapter provided limitation of the research and directions for future research.

REFERENCES

Ackermann T., Widjaja T., Benlian A., Buxmann P., (2012, December), ‘Perceived IT Security Risk of Cloud Computing’, 33rd International Conference on Information Systems, Orlando, United States of America, December 16-19, pp. 2-4

Belanger F., (2011), ‘Privacy in the Digital Age: A review of Information privacy research in Information systems’, *MIS Quarterly*, Vol. 35, No.4, pp. 1017-1041

Bisong A., Rahman S., (2011), ‘An overview of the security concern in enterprise cloud computing’, *International journal of network security & its applications* (IJNSA), Vol.3, No.1, pp. 36

Boss S., Kirsch L, (2007, December), ‘The Last Line of defence: Motivating Employees to follow corporate security guidelines’, Twenty Eighth International Conference on Information Systems, ICIS 2007 Proceedings. 103, Montreal, Quebec, Canada, December 9-12, pp. 3-5

Cerf V., (2010), ‘Despite Its Age, The Internet is Still Filled with Problems’, https://readwrite.com/2009/02/15/vint_cerf_despite_its_age_the/, Accessed date 05-Mar-2018, pp. 3-5

Chen P., Zhang C., (2014), ‘Data Intensive Applications, challenges, techniques and technologies: A survey on Big Data’, *Information Sciences*, 275:314–347, pp. 314-347, doi: 10.1016/j.ins.2014.01.015

Cloud Security Alliance CSA, (2016), ‘The Treacherous 12, Cloud Computing Top threats in 2016’, https://cloudsecurityalliance.org/group/top-threats/, Accessed date 07-Feb-2017, pp. 7-35

Naydenov R., Liveri D., Dupre L., Chalvatzi E. , (2015), ‘Secure use of cloud computing in the finance sector, Good Practices and recommendations’, *European network for network and information security* (ENISA), pp. 7-36, ISBN 978-92-9204-138-0, DOI 10.2824/199301

Fisher E., (2016), ‘Cyber security challenges: In brief’, *Congressional Research Service*, 7-5700, www.crs.gov, R43831, pp. 2

Foley J., (2008), ‘Private Clouds Take Shape, Information Week’, retrieved from, https://www.informationweek.com/private-clouds-take-shape/d/d-id/1070793, Accessed date 06-SEP-2017, pp. 1

Gupta A., Zhdanov D., (2012), ‘Growth and sustainability of managed security services network: An economic perspective’, Department of operations and decision sciences, Carlos school of management, University of Minnesota, *MIS Quarterly*, Research Article, Vol.36, No.4, pp. 1109-1130

Hashizume K., Rosado D., Madina E., Fernandez E., (2013), ‘An analysis of security issue in cloud computing’, *Journal of internet services and application*, 2013 4:5, available at http://www.jisajournal.com/content/4/1/5, pp. 1-13

Nwogu E., (2014), ‘Improving security of interest banking system using three–level security implementation’, *IRACST – International Journal of computer science and information technology & security* (IJCSITS), ISSN: 2249-9555, Vol.4, No.6, pp. 168-169

Qian L, Leigh L., Quarterman, John S., Whinston, A., (2012, December), ‘Reputation as public policy for internet security: A field study’, Thirty third international conference on information systems, Orlando, United States of America, December 16-19, pp. 4-6

Rouse M., (2014), ‘What is public cloud? Whatis.com’, https://searchcloudcomputing.techtarget.com/definition/cloud-infrastructure, 20-Oct-2017, pp. 1-3

Sun Y, Zhang J., Xiong Y, and Zhu G., (2014), ‘Review Article on Data Security and Privacy in Cloud Computing’, *International Journal of Distributed Sensor Networks*, IJDSN, Vol. 10, Issue 72014, ISSN: 190903, pp. 1-9, https://doi.org/10.1155/2014/190903

Uffen J., Guhr N., Brietner M, (2012), ‘Personality trait and information security management: An imperial study of information security executives’, 33rd International Conference on Information Systems, Orlando, United States of America, pp. 4-5

Won K., (2009), ‘Cloud Computing: Today and Tomorrow’, *Journal of Object Technology*, Vol. 8, No. 1, pp. 3-4

Yakoubov S., Gadepally V., Schear N., Shen E., Yerukhimovich A., (2014, September), ‘A survey of Cryptographic approaches to securing Big-Data Analytics in Cloud’, 2014 IEEE High Performance Extreme Computing Conference (HPEC’14), Waltham, MA USA, September 9-11, pp. 2, doi: 10.1109/HPEC.2014.7040943

Zissis D., Lekkas D., (2010), ‘Addressing Cloud computing security issues’, Future generation computer systems 28, Vol. 28, pp. 583-592,

In Yang, Hongji; Liu, Xiaodong, (2014), ‘Understanding Cloud Computing’, *Hershey, PA: Information Science*, pp. 204–227

Peter Mell and Timothy Grance, (2014), ‘The NIST Definition of Cloud Computing (Technical report). National Institute of Standards and Technology: U.S. Department of Commerce’, *NIST Special publication*, September 2014, pp. 2-3

Ackermann et. al., (2012), ‘Perceived IT Security Risk of Cloud Computing’, 33rd, International Conference on Information Systems, pp. 3

Alok Gupta, Dmitry Zhdanov, (2012), ‘Growth and sustainability of managed security services network: An economic perspective’, *MIS Quarterly Research*, vol.36, No.4, pp. 1109-1130

Daniyal M. Algazzawi, Sydem Hamid Hasan, Mohhamad Slim Trigui , (2014), ‘Information systems threats and vulnerabilities’, *International Journal of computing applications*, Volume 89, No.03, pp. 1-7

Keiko Hashizume, David G Rosado, Eduardo Fernandez Madina, Eduaro B Fernandez, (2013), ‘An analysis of security issue in cloud computing, *Journal of internet services and application*, pp.1-13

Analysis of Internet Users’ Level of Online Privacy Concerns, Dara O’Neil, Georgia Institute of Technology, *Social Science Computer Review*, Vol. 19 No. 1, Spring 2001, 17-31.

Cohen, J.E., (2013), ‘What is Privacy for?’, *Harvard Law Review*, 126.

Coombs, K.A. (2005), ‘Protecting USER PRIVACY in the Age of DIGITAL LIBRARIES’, *Computers in Libraries*, vol.25, no. 6, pp. 16-20.

Martins de Andrade P., Albuquerque A., Dourado W., Aguiar da Silva F., (2016), ‘Change Management: Implementation and Benefits of the change control in the information Technology Environment’, *International Journal of Advanced Information Technology* (IJAIT) Vol. 6, No. 1, pp. 1-11

Anantharaman N., (2018), ‘Agile Incident Management using Kanban Board for data Visualization’, *IOSR Journal of Computer Engineering* (IOSR-JCE), vol. 17, pp.17-20

Sebaaoui S., Lamrini M., (2012), ‘Implementation of ITIL in a Moroccan company: the case of incident management process’, *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 4, No 3, pp. 1-7

Jäntti M., Cater-Steel A., (2017), ‘Proactive Management of IT Operations to improve IT Services’, *JISTEM - Journal of Information Systems and Technology Management*, Vol. 14, No. 2, pp. 191-218

Talla M., Valverde R., (2013), ‘An Implementation of ITIL Guidelines for IT Support Process in a Service Organization’, *International Journal of Information and Electronics Engineering*, Vol. 3, No. 3, pp 1-7

Talla M., Valverde R., (2013), ‘An Implementation of ITIL Guidelines for IT Support Process in a Service Organization’, *International Journal of Information and Electronics Engineering*, Vol. 3, No. 3, pp. 1-7

Merrill Warkentin and Robert Willison, (2009), ‘Behavioural and policy issues in information systems security: the insider threat’, *European Journal of Information Systems*, vol. 18, pp. 101–105

Mahalle A., Yong J., Tao X., (2021), 'Challenges and Mitigation for Application Deployment over SaaS Platform in Banking and Financial Services Industry', IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China, pp. 1-6

Mahalle A., Yong J., Tao X., (2021), 'Regulatory Challenges and Mitigation for Account Services Offered by FinTech', 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China, pp. , pp. 1-6

Mahalle A., Yong J., Tao X., (2020), 'IT Investment Governance and Corporate Governance: Perspective and Approach', 7th International Conference on Behavioural and Social Computing (BESC), Bournemouth, UK, pp. 1-6

Mahalle A., Yong J., Tao X., (2019), 'Protecting Privacy in Digital Era on Cloud Architecture for Banking and Financial Services Industry', 6th International Conference on Behavioral, Economic and Socio-Cultural Computing (BESC), Beijing, China, pp. 1-6

Mahalle A., Yong J., Tao X., (2019), 'Ethics of IT Security Team for Cloud Architecture Infrastructure in Banking and Financial Services Industry', 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal, pp. 1-6

Mahalle A., Yong J., Tao X., (2019), 'Insider Threat and Mitigation for Cloud Architecture Infrastructure in Banking and Financial Services Industry', 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Porto, Portugal, pp. 1-6

Mahalle A., Yong J., Tao X., (2018), 'ITIL Processes to Control Operational Risk in Cloud Architecture Infrastructure for Banking and Financial Services Industry', 5th International Conference on Behavioral, Economic, and Socio-Cultural Computing (BESC), Kaohsiung, Taiwan, pp.1-6

Mahalle A., Yong J., Tao X., Shen J., (2018), 'Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure', 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanjing, China, pp. 1-6

LIST OF APPENDICES

Appendix A. Online survey questions and relation to research questions

Research Questions: Cloud Governance

Question No.	Question Description	Research Question (RQ) No.	Research Area
1	What is the method to design Cloud governance framework?	RQ2	Cloud Governance
2	Who are accountable people for cloud governance?)	RQ1	Cloud Governance
3	What are communication channels, methods, and frequency of cloud governance problems?	RQ2	Cloud Governance
4	What is area of re-design for cloud improvements?	RQ1	Cloud Governance
5	What are key parameters of Cloud Score Card / Cloud Operational Excellence?	RQ1	Cloud Governance
6	What are areas of cloud computing that confirms the value delivery to business?	RQ1	Cloud Governance
7	What are areas of Cloud improvement investment?	RQ1	Cloud Governance
8	How data categorization over cloud and its governance is related?	RQ1	Cloud Governance
9	What is governance structure for Cloud due to digital transformation?	RQ4	Cloud Governance
10	How are cloud development and its objectives related with data security?	RQ2	Cloud Governance
11	How are cloud development and its objectives related with system security?	RQ2	Cloud Governance
12	How are roles and responsibilities of cloud governance teams segregated?	RQ3	Cloud Governance
13	How control over system changes to cloud architecture are controlled?	RQ2	Cloud Governance
14	How is cloud maturity model evaluated with change in architecture?	RQ1	Cloud Governance

Question No.	Question Description	Research Question (RQ) No.	Research Area
15	How often skills and expertise of cloud service provider and cloud support team is evaluated?	RQ3	Cloud Governance
16	How do you differentiate between governance needs of application, process, people, and infrastructure?	RQ2	Cloud Governance
17	How Cloud governance framework monitors and controls third party vendors and contractors?	RQ2	Cloud Governance
18	On the scale of 1 to 10 (1 being lowest and 10 being highest) will you rate effectiveness of cloud governance for cloud operability?	RQ1	Cloud Governance
19	How are roles and responsibilities of various team aligning to Cloud value delivery?	RQ2	Cloud Governance
20	How needs of specialised team like Forensic investigation, customer experience platforms, regulatory bodies are addressed through cloud governance?	RQ5	Cloud Governance
21	Do you evaluate existing governance framework and its effectiveness?	RQ2	Cloud Governance
22	How do you evaluate existing governance framework and its effectiveness?	RQ2	Cloud Governance
23	Do you have clear strategic plan to assess data security and system security at governance forum?	RQ1, RQ2	Cloud Governance
24	Does project portfolio management office (PPMO) clearly define, evaluates, prioritise, selects, initiates, manages and controls data and system security related changes as a part of project delivery?	R1, RQ2	Cloud Governance
25	Does enterprise information architecture model support creation, use and sharing of data by users in a way to maintain integrity and is secure from failures?	RQ1	Cloud Governance

Question No.	Question Description	Research Question (RQ) No.	Research Area
26	How do you manage integrity of data stored in electronic form such as databases, data warehouse and data archives?	RQ1, RQ2	Cloud Governance
27	Does technological direction and adoption addresses systems architecture, migration strategies and contingency aspects of data and system security?	RQ1, RQ2	Cloud Governance
28	Who governs and addresses the issue arising out of technological changes that poses threat to data and system security?	RQ1, RQ2, RQ3	Cloud Governance
29	How does IT process management framework addresses data and system security?	RQ1, RQ2	Cloud Governance
30	Do you have dedicated budget and investment management framework to support Data and system security?	RQ1, RQ2, RQ3	Cloud Governance
31	How does Enterprise IT Risk and control framework addresses issue of data and system security?	RQ1, RQ2	Cloud Governance
32	How do you educate, train, and develop IT Staff for data and system security?	RQ1, RQ2	Cloud Governance
33	How do you assess quality of data and system security?	RQ1, RQ2	Cloud Governance
34	What are steps to manage and control the risk related events identified for data and system security?	RQ1, RQ2, RQ3, RQ4	Cloud Governance
35	How do you protect technological infrastructure (physically) to prevent loss of data and threat to information system security?	RQ1, RQ2	Cloud Governance
36	How do you control the IT contracts of projects and operations to confirm data and systems security?	RQ1, RQ2	Cloud Governance

Question No.	Question Description	Research Question (RQ) No.	Research Area
37	How do you keep control over emergency changes to mitigate risk of system downtime and resolve high impact incidents?	RQ1, RQ2, RQ3, RQ4	Cloud Governance
38	Are there any specific service level agreements (SLAs) in business usual activities that cover data and system security related aspects?	RQ1, RQ2	Cloud Governance
39	As a part of business continuity plans, do you identify and reserve resources within team who deal with data and system security?	RQ1, RQ2, RQ3	Cloud Governance
40	Does your IT Security plan include data and system security specific controls?	RQ1, RQ2, RQ3, RQ4	Cloud Governance
41	Are service desk agents are educated, trained and skilled to record, report and respond to incidents raised for data and system security breach?	RQ1, RQ2	Cloud Governance
42	How do you ensure the monitoring in everyday operations?	RQ1, RQ2, RQ3	Cloud Governance
43	On the scale of 1 to 10, (10 being very complex) how complex you see monitoring and managing cloud hosted via 3rd party contractor?	RQ1, RQ2	Cloud Governance

Research Questions: Cloud Security

Question No.	Question Description	Research Question (RQ) No.	Research Area
1	What is most important area in IT security implementation?	RQ1	Cloud Security
2	What are most important areas of security breach incidents related to data?	RQ1	Cloud Security
3	What are security perimeter controls to monitor data leakages?	RQ1	Cloud Security
4	What are penetration testing cases to cover data security?	RQ2	Cloud Security
5	What are penetration testing cases to cover system security?	RQ2	Cloud Security
6	Are vulnerability assessment tools sufficient to report data security related incidents?	RQ2	Cloud Security
7	Are vulnerability assessment tools sufficient to report data security related incidents through digital platforms?	RQ4	Cloud Security
8	Is there any independent governance framework for data and system security?	RQ2	Cloud Security
9	What are bank specific security enforcement point to confirm data security?	RQ2	Cloud Security
10	Do you classify data based on data type?) Example: PII, Card Information, Transaction processing)	RQ2	Cloud Security
11	Does data categorization help to minimise risk of data loss?	RQ2	Cloud Security
12	Have you recently added / updated data security tools to meet existing threats and vulnerabilities?	RQ2	Cloud Security
13	Is IT security team informed about actions required to prevent data leakages?	RQ3	Cloud Security
14	Has digital transformation added new data leakages areas?	RQ4	Cloud Security

Question No.	Question Description	Research Question (RQ) No.	Research Area
15	Do you have process and tools in place to recover hardware and devices in case specific department asks for its?	RQ5	Cloud Security
16	Do you conduct regular training program with staff and 3rd Party vendors to bring awareness about data security?	RQ2	Cloud Security
17	How do you handle cyber-attack or DDoS?	RQ2	Cloud Security
18	Do you share findings of intrusion protection system (IPS) with other organizations / Banks?	RQ2	Cloud Security
19	What Bank specific parameters are considered while configuring data leakage prevention tools?	RQ2, RQ4	Cloud Security
20	Do you have dedicated team to handle security policy compliance and incidents?	RQ1, RQ2	Cloud Security
21	Are traffic monitoring tools sufficient to filter packet level information?	RQ2	Cloud Security
22	Does traffic monitoring tool help monitor users from all channels?	RQ2, RQ4	Cloud Security
23	Do you define the encryption methods based on data type?	RQ1	Cloud Security
24	What is the frequency to update Security Certificates (SSL)?	RQ1, RQ2, RQ4	Cloud Security
25	What is the frequency to upgrade monitoring and alert mechanism?	RQ1, RQ2, RQ4	Cloud Security
26	What are the methods to manage Identity and access management (IAM) for cloud infrastructure?	RQ1, RQ2	Cloud Security
27	Do you have Risk event and risk mitigation plan in case of cyber-attack or threat detection cases?	RQ1, RQ2, RQ3, RQ4	Cloud Security

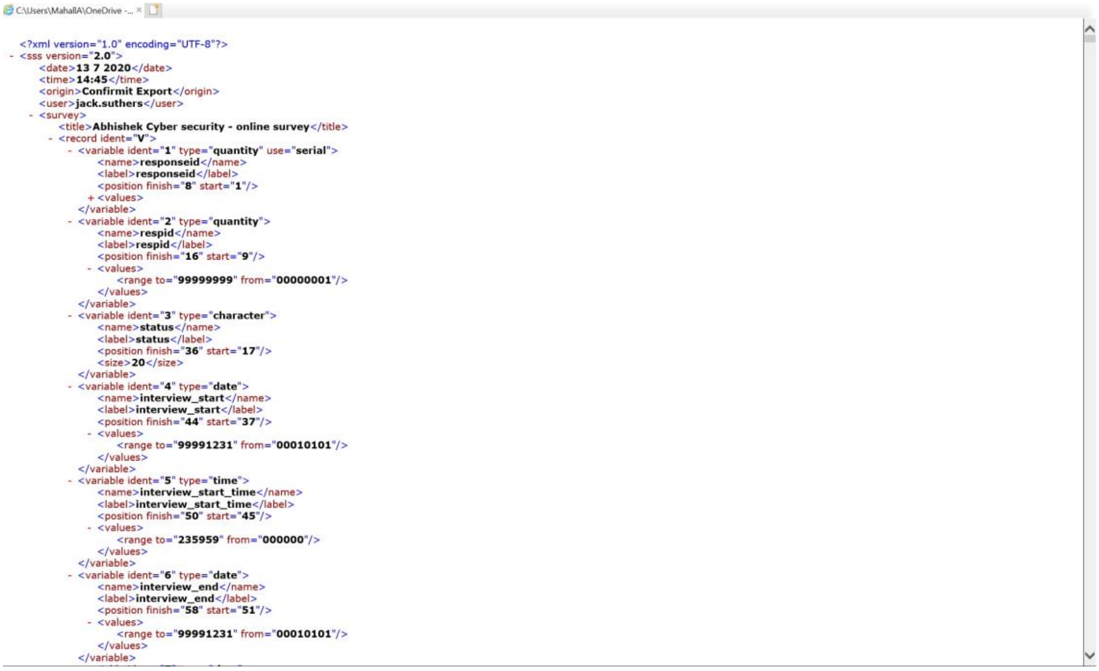
Question No.	Question Description	Research Question (RQ) No.	Research Area
28	Do you have dedicated high severity incident management and response team?	RQ1, RQ2	Cloud Security
29	Do you monitor and log user activities?	RQ1, RQ2, RQ4	Cloud Security
30	Do you plan OR have you implemented machine learning and Artificial intelligence to respond to suspicious activities by internal or external users?	RQ1, RQ2, RQ3, RQ4	Cloud Security
31	Is there any defined process to action against suspicious behaviour in network security perimeter? (User logging, Intrusion identification, account hijacking, password failures)	RQ1, RQ2	Cloud Security
32	What is the mechanism to identify malicious code injection or script run on desktops, servers, storage drives and resources on cloud?	RQ1, RQ2	Cloud Security
33	Do you have data retention tools?	RQ2	Cloud Security
34	What are methods for data deletion for lost devices?	RQ1, RQ2, RQ4, RQ5	Cloud Security
35	Is there a defined process to handle compromised devices?	RQ2	Cloud Security
36	Is there a repository of antimalware identified to develop Bank's defence system secure from similar attack in future?	RQ1, RQ2	Cloud Security
37	Is there any defined process to handle 3rd Party System Users?	RQ1, RQ2, RQ4	Cloud Security
38	Have you defined key risk parameters for cloud infrastructure resources?	RQ1, RQ2, RQ4	Cloud Security
39	Is there a job rotation within IT security team?	RQ1, RQ2, RQ4	Cloud Security
40	Do you schedule employee and 3rd Party education programs for cloud security?	RQ1, RQ2, RQ3	Cloud Security

Question No.	Question Description	Research Question (RQ) No.	Research Area
41	Who is responsible for physical security of data centre?	RQ1, RQ2	Cloud Security
42	Who is responsible for cloud user back-ground checks?	RQ2	Cloud Security
43	How do you ensure audit and compliance requirement for cloud security?	RQ1, RQ2, RQ3	Cloud Security
44	Are IT Security contracts separate from Enterprise IT Contracts?	RQ1, RQ2, RQ3, RQ4, RQ5	Cloud Security
45	How do you monitor and govern test environments and production environments over cloud infrastructure?	RQ1, RQ2, RQ3, RQ4	Cloud Security
46	How do you monitor, measure, and maintain ethical controls within team to ensure culture of trust and responsibility within team?	RQ1, RQ2, RQ3	Cloud Security
47	How are you supporting the digital transformation across Bank?	RQ1, RQ2, RQ5	Cloud Security
48	Do you see need to share information about cyber-attack or potential threat with other Banks to improve security and bring shared knowledge to a common platform?	RQ1, RQ2	Cloud Security
49	Has cloud computing added more risk to Bank?	RQ1, RQ2	Cloud Security

Research Questions: Cloud Perception

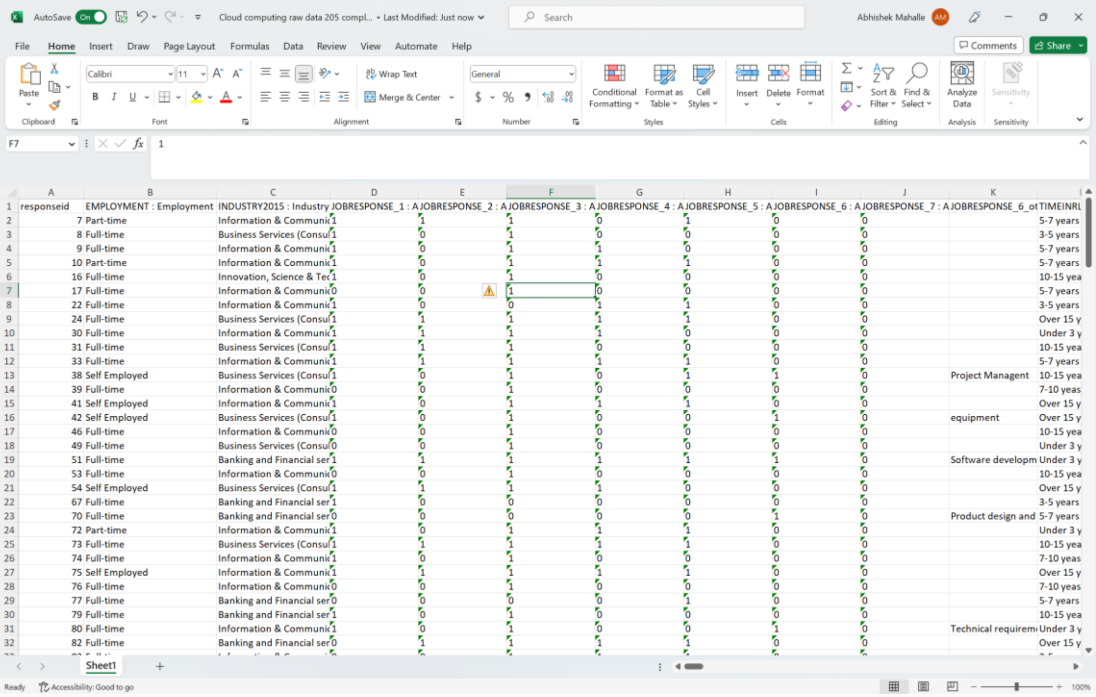
Question No.	Question Description	Interview Question No.	Research Area
1	Ease of Use	1	Cloud Perception
2	Flexibility to work from Home	2	Cloud Perception
3	Data confidentiality and information security maintained	3	Cloud Perception
4	Simple to connect	4	Cloud Perception
5	Availability of all computing resources	5	Cloud Perception
6	Secure to connect from private network	6	Cloud Perception
7	Ability to recover data in case of loss	7	Cloud Perception
8	Support from remotely located teams in case of incidents	8	Cloud Perception

Appendix B. XML format of survey



```
  <?xml version="1.0" encoding="UTF-8"?>
- <sss version="2.0">
      <date>13 7 2020</date>
      <time>14:45</time>
      <origin>Confirmit Export</origin>
      <user>jack.suthers</user>
    - <survey>
          <title>Abhishek Cyber security - online survey</title>
        - <record ident="V">
            - <variable ident="1" type="quantity" use="serial">
                  <name>responseid</name>
                  <label>responseid</label>
                  <position finish="8" start="1"/>
                + <values>
              </variable>
            - <variable ident="2" type="quantity">
                  <name>respid</name>
                  <label>respid</label>
                  <position finish="16" start="9"/>
                - <values>
                      <range to="99999999" from="00000001"/>
                  </values>
              </variable>
            - <variable ident="3" type="character">
                  <name>status</name>
                  <label>status</label>
                  <position finish="36" start="17"/>
                  <size>20</size>
              </variable>
            - <variable ident="4" type="date">
                  <name>interview_start</name>
                  <label>interview_start</label>
                  <position finish="44" start="37"/>
                - <values>
                      <range to="99991231" from="00010101"/>
                  </values>
              </variable>
            - <variable ident="5" type="time">
                  <name>interview_start_time</name>
                  <label>interview_start_time</label>
                  <position finish="50" start="45"/>
                - <values>
                      <range to="235959" from="000000"/>
                  </values>
              </variable>
            - <variable ident="6" type="date">
                  <name>interview_end</name>
                  <label>interview_end</label>
                  <position finish="58" start="51"/>
                - <values>
                      <range to="99991231" from="00010101"/>
                  </values>
              </variable>
```

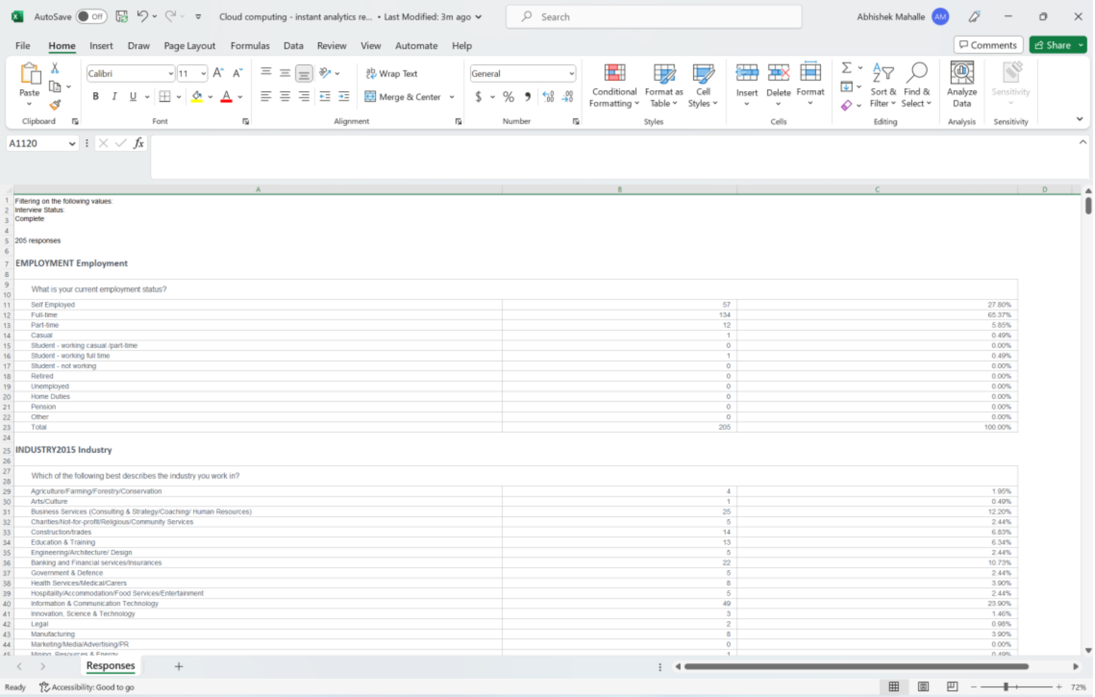
Appendix C. Survey questionnaires



responseid	EMPLOYMENT : Employment	INDUSTRY2015 : Industry	JOBRESPONSE_1 : A	JOBRESPONSE_2 : A	JOBRESPONSE_3 : A	JOBRESPONSE_4 : A	JOBRESPONSE_5 : A	JOBRESPONSE_6 : A	JOBRESPONSE_7 : A	JOBRESPONSE_6_ot	TIMEINRL
7	Part-time	Information & Communic	1	1	1	0	1	0	0		5-7 years
8	Full-time	Business Services (Consul	1	0	1	0	0	0	0		3-5 years
9	Full-time	Information & Communic	1	0	1	1	0	0	0		5-7 years
10	Part-time	Information & Communic	1	0	1	1	1	0	0		5-7 years
16	Full-time	Innovation, Science & Tec	1	0	1	0	0	0	0		10-15 yea
17	Full-time	Information & Communic	0	0	1	0	0	0	0		5-7 years
22	Full-time	Information & Communic	1	0	0	1	1	0	0		3-5 years
24	Full-time	Business Services (Consul	1	1	1	1	1	0	0		Over 15 y
30	Full-time	Information & Communic	1	1	1	1	0	0	0		Under 3 y
31	Full-time	Business Services (Consul	1	1	1	0	0	0	0		10-15 yea
33	Full-time	Information & Communic	1	1	1	1	1	0	0		5-7 years
38	Self Employed	Business Services (Consul	1	0	1	0	1	1	0	Project Managent	10-15 yea
39	Full-time	Information & Communic	0	0	1	0	0	0	0		7-10 yeas
41	Self Employed	Information & Communic	1	0	1	1	1	0	0		Over 15 y
42	Self Employed	Business Services (Consul	1	0	1	0	0	1	0	equipment	Over 15 y
46	Full-time	Information & Communic	0	0	1	0	0	0	0		10-15 yea
49	Full-time	Business Services (Consul	0	0	1	0	0	0	0		Under 3 y
51	Full-time	Banking and Financial ser	1	1	1	1	1	1	0	Software developm	Under 3 y
53	Full-time	Information & Communic	0	0	1	0	0	0	0		10-15 yea
54	Self Employed	Business Services (Consul	1	1	1	1	0	0	0		Over 15 y
67	Full-time	Banking and Financial ser	1	0	0	0	0	0	0		3-5 years
70	Full-time	Banking and Financial ser	0	0	0	0	0	1	0	Product design and	5-7 years
72	Part-time	Information & Communic	1	0	1	1	1	0	0		Under 3 y
73	Full-time	Business Services (Consul	1	1	1	1	1	0	0		10-15 yea
74	Full-time	Information & Communic	1	0	1	0	0	0	0		7-10 yeas
75	Self Employed	Information & Communic	1	1	1	1	1	0	0		Over 15 y
76	Full-time	Information & Communic	0	0	1	0	0	0	0		7-10 yeas
77	Full-time	Banking and Financial ser	0	0	0	0	1	0	0		5-7 years
79	Full-time	Banking and Financial ser	1	0	1	0	0	0	0		10-15 yea
80	Full-time	Information & Communic	1	0	1	0	0	1	0	Technical requirem	Under 3 y
82	Full-time	Banking and Financial ser	0	1	1	1	1	0	0		Over 15 y

AutoSave On
Cloud computing raw data 205 compl... • Last Modified: Just now
Search
Abhishek Mahalle
File Home Insert Draw Page Layout Formulas Data Review View Automate Help
Comments Share
F7
1
Sheet1
Ready Accessibility: Good to go
100%

Appendix D. Survey analytics



Filtering on the following values:
Interview Status:
Complete

205 responses

EMPLOYMENT Employment

What is your current employment status?

Self Employed	57	27.80%
Full-time	134	65.37%
Part-time	12	5.85%
Casual	1	0.49%
Student - working casual /part-time	0	0.00%
Student - working full time	1	0.49%
Student - not working	0	0.00%
Retired	0	0.00%
Unemployed	0	0.00%
Home Duties	0	0.00%
Pension	0	0.00%
Other	0	0.00%
Total	205	100.00%

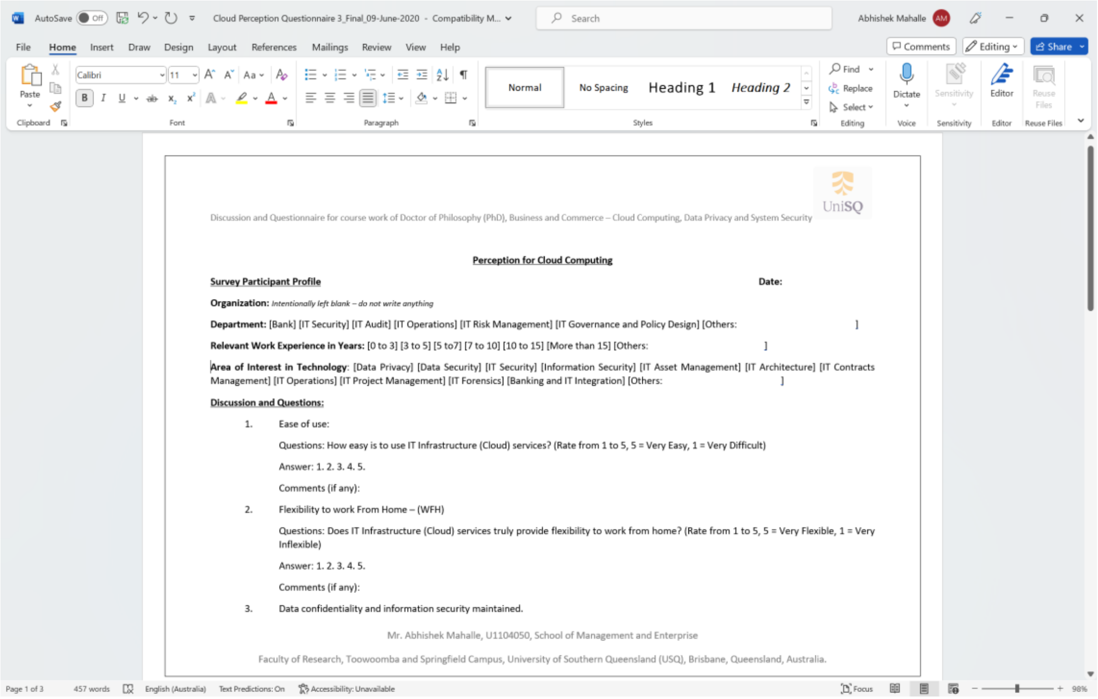
INDUSTRY2015 Industry

Which of the following best describes the industry you work in?

Agriculture/Farming/Forestry/Conservation	4	1.95%
Arts/Culture	1	0.49%
Business Services (Consulting & Strategy/Coaching/ Human Resources)	25	12.20%
Charities/Not-for-profit/Religious/Community Services	5	2.44%
Construction/trades	14	6.83%
Education & Training	13	6.34%
Engineering/Architecture/ Design	5	2.44%
Banking and Financial services/Insurances	22	10.73%
Government & Defence	5	2.44%
Health Services/Medical/Carers	8	3.90%
Hospitality/Accommodation/Food Services/Entertainment	5	2.44%
Information & Communication Technology	49	23.90%
Innovation, Science & Technology	3	1.46%
Legal	2	0.98%
Manufacturing	8	3.90%
Marketing/Media/Advertising/PR	0	0.00%

AutoSave Off
Cloud computing - instant analytics re... • Last Modified: 3m ago
Search
Abhishek Mahalle
File Home Insert Draw Page Layout Formulas Data Review View Automate Help
Comments Share
A1120
Responses
Ready Accessibility: Good to go
72%

Appendix E. Interview questionnaires on perception on cloud computing



Discussion and Questionnaire for course work of Doctor of Philosophy (PhD), Business and Commerce – Cloud Computing, Data Privacy and System Security

UniSQ

Perception for Cloud Computing

Survey Participant Profile **Date:**

Organization: *Intentionally left blank – do not write anything*

Department: [Bank] [IT Security] [IT Audit] [IT Operations] [IT Risk Management] [IT Governance and Policy Design] [Others:]

Relevant Work Experience in Years: [0 to 3] [3 to 5] [5 to7] [7 to 10] [10 to 15] [More than 15] [Others:]

Area of Interest in Technology: [Data Privacy] [Data Security] [IT Security] [Information Security] [IT Asset Management] [IT Architecture] [IT Contracts Management] [IT Operations] [IT Project Management] [IT Forensics] [Banking and IT Integration] [Others:]

Discussion and Questions:

1. Ease of use:

   Questions: How easy is to use IT Infrastructure (Cloud) services? (Rate from 1 to 5, 5 = Very Easy, 1 = Very Difficult)

   Answer: 1. 2. 3. 4. 5.

   Comments (if any):

2. Flexibility to work From Home – (WFH)

   Questions: Does IT Infrastructure (Cloud) services truly provide flexibility to work from home? (Rate from 1 to 5, 5 = Very Flexible, 1 = Very Inflexible)

   Answer: 1. 2. 3. 4. 5.

   Comments (if any):

3. Data confidentiality and information security maintained.

Mr. Abhishek Mahalle, U1104050, School of Management and Enterprise

Faculty of Research, Toowoomba and Springfield Campus, University of Southern Queensland (USQ), Brisbane, Queensland, Australia.